S. Hrg. 99-915

COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1986

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT OF GOVERNMENT MANAGEMENT

OF THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

NINETY-NINTH CONGRESS

SECOND SESSION

ON

S. 2756

TO AMEND TITLE 5 OF THE UNITED STATES CODE, TO ENSURE PRIVACY, AND VERIFICATION OF DATA DISCLOSED FOR COMPUTER MATCHING, TO ESTABLISH DATA INTEGRITY BOARDS WITHIN FEDERAL AGENCIES, AND FOR OTHER PURPOSES

SEPTEMBER 16, 1986

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE
64-697 O WASHINGTON : 1986

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

S401-12

COMMITTEE ON GOVERNMENTAL AFFAIRS

WILLIAM V. ROTH, Jr., Delaware, *Chairman*

TED STEVENS, Alaska
CHARLES McC. MATHIAS, Jr., Maryland
WILLIAM S. COHEN, Maine
DAVE DURENBERGER, Minnesota
WARREN B. RUDMAN, New Hampshire
THAD COCHRAN, Mississippi

THOMAS F. EAGLETON, Missouri
LAWTON CHILES, Florida
SAM NUNN, Georgia
JOHN GLENN, Ohio
CARL LEVIN, Michigan
ALBERT GORE, Jr., Tennessee

Franklin G. Polk, *Chief Counsel and Staff Director*
Gary Zizka, *Minority Staff Director*

Subcommittee on Oversight of Government Management

WILLIAM S. COHEN, Maine, *Chairman*

WARREN B. RUDMAN, New Hampshire
DAVE DURENBERGER, Minnesota

CARL LEVIN, Michigan
LAWTON CHILES, Florida

Susan M. Collins, *Staff Director*
Mary B. Gerwin, *Counsel*
Frances C. de Vergie, *Chief Clerk*

CONTENTS

Page

Opening statements:
  Senator Cohen 1
  Senator Durenberger 3
  Senator Levin 14

WITNESSES

Tuesday, September 16, 1986

Joseph R. Wright, Jr., Deputy Director, Office of Management and Budget, and Richard P. Kusserow, Inspector General, Department of Health and Human Services 4
Joseph F. Delfico, Senior Associate Director, Human Resources Division, General Accounting Office, accompanied by David Pasquarello, evaluator, (Philadelphia office); Richard Halter, assignment manager (Philadelphia region); and Daniel Brier, group director, Human Resources Division 21
Ronald L. Plesser, American Bar Association 26
Jerry J. Berman, chief legislative counsel, American Civil Liberties Union 32
Priscilla M. Regan, Ph.D., Office of Technology Assessment 39

Alphabetical List of Witnesses

Berman, Jerry J.:
  Testimony 32
  Prepared statement 104
Brier, Daniel: Testimony 21
Delfico, Joseph F.:
  Testimony 21
  Prepared statement with attachments 77
Halter, Richard: Testimony 21
Kusserow, Richard P.: Testimony 4
Pasquarello, David: Testimony 21
Plesser, Ronald L.:
  Testimony 26
  Prepared statement 92
Regan, Priscilla M., Ph.D.:
  Testimony 39
  Prepared statement 125
Wright, Joseph R., Jr.:
  Testimony 4
  Prepared statement 47

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Prepared statements of witnesses 47
Text of S. 2756 141
Office of Management and Budget, Revised Guidance for Conducting Computer Matching Programs, May 19, 1982 (47 FR 21[illegible]56) 152
Office of Management and Budget, Computer Match Checklist and Model Control System and Resource Document for Conducting Computer Matching Projects Involving Individual Privacy Data, December 29, 1983 154
Letter from Senator William S. Cohen to the Honorable Joseph R. Wright, Jr., Deputy Director, Office of Management and Budget, September 19, 1986 233

Page

Letter from the Honorable Joseph R. Wright, Jr., Deputy Director, Office of Management and Budget, to Senator William S. Cohen, October 7, 1986 234

Catalog of Automated Front-End Eligibility Verification Techniques, Project of the President's Council on Integrity and Efficiency, September 1985 247

"Survey of State Implementation of the Income and Eligibility Provisions of the 1984 Deficit Reduction Act," U.S. General Accounting Office, September 1986 301

Executive summary, "Privacy Act: Federal Agencies' Implementation Can Be Improved," U.S. General Accounting Office, August 1986 322

Computer matching focus paper, American Civil Liberties Union Privacy and Technology Project, September 1985 326

Summary, "Federal Government Information Technology: Electronic Record Systems and Individual Privacy," Office of Technology Assessment, June 1986 340

Statement of the National Association of Tax Administrators on S. 2756 and its effects on the Federal-State tax exchange program 347

Statement of Hugh V. O'Neill on S. 2756, the Computer Matching and Privacy Protection Act of 1986 352

COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1986

TUESDAY, SEPTEMBER 16, 1986

U.S. Senate,
Subcommittee on Oversight
of Government Management,
Committee on Governmental Affairs,
Washington, DC.

The subcommittee met at 9:30 a.m. in room SD-342 of the Dirksen Senate Office Building, Hon. William S. Cohen, chairman of subcommittee, presiding.

Present: Senators Cohen, Durenberger, and Levin.

Staff present: Susan M. Collins, staff director; Mary B. Gerwin, counsel; Linda J. Gustitus, minority staff director and chief counsel to the minority; Elise J. Bean, minority counsel; and Frankie de Vergie, chief clerk.

OPENING STATEMENT OF SENATOR COHEN

Senator Cohen. The committee will come to order.

Over the past 4 years, this subcommittee has watched the explosive growth of computer matching at both the Federal and State levels of government. In matching programs, agencies routinely exchange and cross check information from two or more data bases, most often to detect fraud, abuse, or overpayments in Government programs.

The Department of Education has, for example, cross checked its lists of delinquent loans with lists of Federal employees to determine whether any student loan defaulters work for the Federal Government. And soon each State agency administering the AFDC, food stamp, and other assistance programs will be matching their lists of applicants and recipients with the IRS files to search for unreported assets or earnings.

The expansion of matching programs over the past few years has been staggering. The Office of Technology Assessment recently estimated that the number of computer matches performed by the Federal Government tripled between 1980 and 1984 with over 2 billion separate records being exchanged during this period. Many of these matches involve very personal information such as income and employment data of individual citizens.

In many instances, computer matching is a useful, efficient tool to protect the integrity of Government programs.

Computer matching programs can also, however, unless properly conducted and controlled, pose serious threats to the privacy and due process rights of individuals whose records are being matched.

The subcommittee's investigation and past hearings have revealed tremendous potential for abuse in computer matching, because there are no mandatory rules for agencies to follow when performing matches, little protection for the person whose records are matched, and inadequate oversight of how these programs are being conducted. Individuals can have crucial Government benefits reduced or terminated solely on the basis of unverified information produced by a computer match, information that can be out-of-date, misleading or just plain wrong. Citizens can be, and have been in the past, placed in the very difficult position of having to defend themselves against information that has never even been reviewed by a human being for its accuracy.

Anyone who has ever done with a computer over a billing error knows how frustrating it can be to prove that the computer has made a mistake. Much more than simple frustration is at stake when essential Government assistance can be cut off because of faulty computer matching results.

The subcommittee is holding this hearing today to consider S. 2756, the Computer Matching and Privacy Protection Act of 1986, legislation which I introduced with Senator Levin. This legislation attempts to strike the proper balance between the legitimate needs of Government efficiency and individual rights.

S. 2756 would require Federal agencies to enter into written agreements before disclosing records for use in computer matching. These agreements would set forth procedures governing the use of the records disclosed for the match itself. The bill would also establish data integrity boards and agencies to ensure better monitoring and review of computer matches. These boards would serve as the principal overseers and policymakers of the agency's implementation of the Privacy Act and will provide more coordinated guidance and training on Privacy Act matters.

The bill before the subcommittee today also insures basic due process protection of individuals whose records are being matched. Specifically, it prohibits agencies from reducing, suspending, or terminating Federal financial assistance on the basis of information produced by a matching program without first verifying the information, giving notice to the individual involved, and providing individuals with an opportunity to refute the information produced by the computer match.

I believe that these basic elements are not only principles of fairness, but they are also good management practices for the agencies to follow.

In calling these hearings, I want to stress that we do not want to reverse the trends of computerization in our society. We must, however, pay adequate attention to the implications of the use of technology and not lose sight of the individual's side of the equation. We must take care not to allow the blessing of technology to become transformed into a beast that will crush the cherished values of democracy.

I recognize that S. 2756 must be developed further to strike the most appropriate balance between the legitimate needs of agencies and individual concerns.

Special consideration, for example, should be given to matching conducted for criminal investigations or national security purposes.

I look forward to working with the Office of Management and Budget, the intelligence agencies, the Inspectors General and advocacy groups to make S. 2756 more workable and to achieve these goals.

Today we are going to hear from witnesses with a variety of views on computer matching.

First, we will hear from Joseph R. Wright, Jr., Deputy Director of the Office of Management and Budget, and Richard P. Kusserow, Inspector General of the Department of Health and Human Services.

We will also hear from the General Accounting Office, the American Bar Association, the American Civil Liberties Union, and the Office of Technology Assessment.

We look forward to the testimony of our witnesses today and thank all of them for their assistance to the subcommittee in our examination of computer matching programs.

So today we welcome our first witness, Joseph Wright, Deputy Director of OMB.

Mr. Wright is also the Chairman of the President's Council on Integrity and Efficiency.

We are also pleased to have with us today Richard Kusserow, Inspector General of the Department of Health and Human Services, who serves as Vice Chairman of the President's Council on Integrity and Efficiency.

Before going on to our two witnesses, Senator Durenberger, would you like to make an opening statement?

OPENING STATEMENT OF SENATOR DURENBERGER

Senator DURENBERGER. Mr. Chairman, thank you very much.

As a member of this subcommittee, I compliment you on holding this hearing to examine whether the use of computer matching programs threatens the privacy rights of individuals. When computerized records are cross-checked by Government agencies, it is important that the rights of individuals be carefully protected.

Computer matching programs provide a way for the government to cross check its records to make sure that individuals are eligible for the benefits they receive. The problem is that sometimes information contained in computer records is wrong or outdated. The result is that individuals can be mistakenly deprived of their government benefits.

The bill you and Senator Levin have introduced strikes an important balance between the rights of individuals to privacy and the needs of Government managers to improve efficiency. It provides information about how agencies are dealing with Privacy Act issues and it recognizes the necessity for greater oversight of computer matching operations.

Perhaps most importantly, it addresses due process concerns by requiring independent verification of information produced by a matching exercise.

I commend both you and Senator Levin on your attention to such an important issue.

While I am pleased with much of S. 2756, and I intend to support it, I believe there are two issues that need to be addressed before the subcommittee takes further action on the bill.

First, I am concerned that the provision that requires notification of the person whose records are to be matched, may be somewhat cumbersome. A notice on the application form used to determine eligibility of program recipients may accomplish the same goal. There may be a less cumbersome alternative.

The second part is related to the verification requirement, which provides individuals with an opportunity to refute the information produced by the match. This requirement is a critical element in S. 2756. I am not clear, however, as to what kinds of administrative procedures would be used to allow individuals to challenge the information produced in the match. I am sure that question, like the previous one, can be easily resolved.

Senator COHEN. Thank you very much, Senator Durenberger.

Before proceeding, I might indicate that Mr. Wright has been most helpful and cooperative in working with Susan Collins and Mary Gerwin of my staff trying to develop this bill. I thank you and Mr. Kusserow for your assistance.

Mr. Wright, would you care to summarize your lengthy statement?

TESTIMONY OF JOSEPH R. WRIGHT, JR., DEPUTY DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET,[1] AND RICHARD P. KUSSEROW, INSPECTOR GENERAL, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. WRIGHT. Thank you, Mr. Chairman.

Both Mr. Kusserow and I are glad to be here this morning. We would like to give you assurance that we will continue to work with you in this important endeavor, because I think we are all trying to achieve the same goal, that is to be able to use computer matching as it was intended, to maintain the privacy of all individuals who would be affected by the activity itself.

I promised you yesterday I would not read my testimony. I will not do so.

I would just like to highlight some of the key points.

Senator COHEN. I did not make the same promise to you.

Mr. WRIGHT. Yes, but you are the chairman. [Laughter.]

The bill, as we see it, clearly authorizes, first of all, the Government's use of computer matching by amending the Privacy Act of 1974 to permit the disclosure of information for matching purposes.

On the other hand, it also requires that these matching programs include a number of procedural due process steps to preserve the rights of the subjects of any matches.

---

[1] See p. 47 for Mr. Wright's prepared statement.

Now a key thing to us, while we do support the basic thrust of the bill, we haven't had a great deal of time to work it all through with your staff. There are some of the areas that we think are troubling.

It is extremely important to all agencies, as well as the Inspector General, to have workable procedures, because we are convinced that because with excessive administrative procedures, we would go into an overkill situation here. If we tried to solve problems that do not exist now, it would damage matching and lead us into the high error rates that we had in the 1970's.

Let me just give you a little bit of a feeling, if I may, as to some of the problems we have. Between 4 and 18 percent of all payments by program go to ineligible persons, depending on the type of programs. But for some of the big ones, for example, AFDC, over a 10-year period of time, 1975 to 1984. The error rate in 1975 was 11.1 percent. It is now down to 6 percent. But the Federal share over that period of time was over $5 billion in errors.

Senator **Cohen**. The Federal share was how much? $5 billion?

Mr. **Wright**. $5 billion, 5-0-8-0 dollars were paid in error. That's AFDC.

On food stamps, between 1975 and 1984, the error rates were 15.9 percent. They've gone to 8.4 percent. During that 10-year period of time, the Federal share of erroneous payments was over $8 billion. In Medicaid, the earliest information we have is 1978, but between 1978 and 1984, the error rate went from 6.6 to 2.7 percent and the Federal share in errors was $2.5 billion.

So even by OMB terms, we're talking about real dollars here. This is something where I believe that with the deficit situation we're facing right now, that it is in the interests of neither the recipients nor the taxpayers nor the Congress and the executive branch to allow these errors to continue.

There has been progress, but there is still a problem. These errors are the kind that computer matching is particularly suited to detect. I feel that Congress has already demonstrated its understanding of the problem and the support for by enacting the Debt Collection Act of 1982, as well as the Deficit Reduction Act of 1984, where they have encouraged agencies to reduce their error rates and their excessive costs through the use of automated matching.

Now back in 1979, OMB issued its guidelines on the conduct of computer matching programs. In the Inspector General Act of 1978, it showed that the directors expected the OMB's matching guideline to be followed by the new inspector generals conducting the matching programs.

I think they have done a pretty good job.

During the 3 years the guidelines were in effect, OMB has received 20 matching reports, but during that time, it was not just the receipt of a typical matching report or a proposal by an agency. OMB and the agencies spent a great deal of time during the process to make sure that the Privacy Act was adhered to.

As a result of that, the guidelines appeared to have satisfied both congressional and public concerns about matching.

The problem is, those early guidelines were unnecessarily expensive. They were administratively difficult to implement. They were hard to understand, and we found toward the end of the 1970's that matching activities tended to diminish substantially.

During this administration the President established the President's Council on Integrity and Efficiency, of which I am the Chairman and Dick Kusserow is the Vice Chairman.

At that time, one of their first projects was to establish the long-term computer matching projects, of which the purposes were to gather and share information on Federal and State matching activities to identify and remove technical and administrative obstacles to computer matching, while preserving the safeguards of personal data and to foster the increase of Federal and State cooperation which is so badly needed in many computer matches.

One of the project's first tasks was to come up with ways to improve those OMB guidelines, and those revised guidelines were issued in May 1982.

Then the PCIE went further and developed a model control systems and resource document for conducting matching projects involving individual privacy data. This provided an approach to make sure that the requirement of the OMB matching guidelines were met and to make sure that adequate protection of personal data was maintained.

Then in December 1983, OMB issued the Computer Match Check List, which is completed by every agency engaged in providing data for computer matching to insure compliance with the Privacy Act and OMB matching guidelines. It is to be completed and maintained for use in annual submissions to OMB and can be read by the GAO, Congress and anybody else to make sure that prudent management positions are made regarding matching and ensuring the safeguarding of the information.

Now Mr. Chairman, there are many examples of what the computer matching benefits have been over the years. I will not go through all of those. I have included many of those in my testimony, but the PCIE has tried to stay on top of this entire computer matching process as well as the Privacy Act. They have come out with Computer Matching Newsletters. That is a quarterly publication. They have come out with standardized formats designed to facilitate State computer matches. They have come out with a manager's guide to computer matching. They have come out with Project Clean data, which is a computer program to increase the integrity of personal files.

In 1981, they came out with a computer security project, which is operated in tandem with the long-term computer matching project.

And I can go on and on. But the main purpose of what I am trying to say is that I believe that the administration has taken the entire computer matching exercise very seriously, along with maintaining the requirements of the Privacy Act.

Now I do go through some lists of problems that we have with the proposed legislation, and I have them in my testimony. I don't think there is any reason to go over them in detail, but like I said before, we agree with the general thrust of what you are trying to do and we will be more than happy to go ahead and work with you.

I was delighted to hear in your statement that there is no intent to put any unnecessary obstacles in the way of doing proper matches for the purpose of reducing waste and fraud in the Government and improving our overall Federal Government management.

Thank you.

Senator COHEN. Thank you very much. Mr. Kusserow, do you have a statement?

Mr. KUSSEROW. No. I am prepared to answer any questions.

Senator COHEN. Let me start asking a question of you, Mr. Wright. As you pointed out, the past computer matching programs have identified millions of dollars in overpayments for fraud in various programs. The mandatory cross checking of files to determine whether the applicants or the recipients are eligible for benefits can also prove fairly costly to agencies, especially state agencies.

After you finish testifying, GAO is going to testify that a majority of the States they surveyed, 29 out of the 43, believe that the costs of matching required by the Deficit Reduction Act may outweigh the benefits of obtaining the tax data itself.

So the question I ask is, do you think that the cost-benefit analysis of matching programs on client eligibility requirements should be required?

Mr. WRIGHT. I think required is probably too strong a word, Mr. Chairman. As you know, in the first OMB guidelines, it was required. The problem that you end up in is that some of the matches, you do not involve savings directly. For example, in the Project Clean data, where you are increasing the accuracy of the files, which I think is in all of our interests, you don't save any direct dollars in those cases.

In many of the law enforcement experiences, we're going on and trying to pick up overpayments in Medicare and Medicaid, and you will never find exactly what the savings are, because many of them come from those who suddenly stop those practices, because you go into prosecution of those who were caught during one of the original matches.

In-general, I believe in cost-benefit analysis, and in this particular area, I think it has to be done with the understanding that in all cases you will not be saving costs, and you will not be gaining revenues as the result of these, but it can be the responsibility, whether it be law enforcement or making sure that the files are accurate, of the Government to go into that.

Senator COHEN. So you don't think that the written matching agreement in this bill should mandate such analysis?

Mr. WRIGHT. No, sir, I do not.

Mr. KUSSEROW. Mr. Chairman, let me add another example along that line.

We do a lot of Medicaid matches. I am going to give you an example of one where I don't think the thrust would be a cost benefit but would be determining how the program is running.

We have a program that we have run in several States where we are looking for pharmacists or physicians that are providing an excessive amount of dangerous drugs to beneficiaries. Certain types of prescriptive drugs that are taken in excess would be harmful to them and not helpful.

In that case we are not looking for ways in which we can cut off any benefits or reduce them. We are looking for doctors that might be overprescribing or a lack of effective controls on the system. That would be for the quality of the program rather than the cost benefit of the program.

Senator COHEN. The quality of which program?

Mr. KUSSEROW. Medicaid. We would be more concerned in that kind of an approach as to whether our beneficiaries are getting too much, let's say, in the way of depressants or stimulants through the prescriptive process. Physicians may not be attentive to the patient's need and actually may prescribe certain types of drugs, or a patient might be going to multiple providers and getting a whole set of different types of prescriptions, the cumulative effect of which would be contrary to their best physical well-being.

Senator COHEN. Do you mean to say that the Department of Health and Human Services is now getting involved in setting up its own medical standards in terms of what is an appropriate level of medical treatment for individuals?

Mr. KUSSEROW. Not at all, but we would go to generally accepted medical standards for certain types of drugs being prescribed. If we find that there is an excess amount of it being prescribed in a certain area, then we bring that to the attention of policymakers and ask them to address what apparently is a vulnerability of the program.

I certainly think it is part of our mandate to ensure quality in delivery of services as well as efficiency in delivery of services.

Senator COHEN. But who determines what an excess or an inappropriate amount of a drug or combination of drugs might be? Who sets that particular standard?

Mr. KUSSEROW. When we do something like that, we always go to the Public Health Service first and foremost and sit down with them, along with the Health Care Finance Administration, to find out whether there is an acceptable standard.

In most cases there are prescriptive standards which are published—and most of them are published by the drug manufacturers—as to what would be an excessive amount for a patient and what they could actually handle. In those circumstances we can see whether or not those standards are being exceeded in some dramatic way which might endanger the beneficiary. If that is the case, then we go back to the program officials and show them the vulnerability and ask them to develop some sort of a prepayment screen or some sort of an examination of the process to reduce that vulnerability.

Senator COHEN. That is news to me. I had never heard of this kind of process of matching being used to set or determine an appropriate level of medical care under the Medicaid Act.

I mean, I can see the justification if you thought some physician was simply trying to prescribe a particular type of drug for a heavy reimbursement from Medicaid, to fatten his own coffers so to speak, but it does seem to me to raise an issue as to whether the Government itself is now setting standards of appropriate medical care.

Mr. KUSSEROW. Absolutely not. In fact, controlled substances do have published standards which should not be exceeded and which if they were would be harmful to a patient.

Senator COHEN. Would you go further and report that particular doctor to the local physicians board in the State, saying, for example, that this individual is engaged in dispensing drugs which are dangerous to the health of his patients?

Mr. KUSSEROW. Yes, in fact we do that. We have a standard policy to report all deviations or apparent deviations from good medical practice to the State licensing authorities.

Senator COHEN. Let me ask you another question. Would that doctor have a chance to refute the statement that you made to the board?

Mr. KUSSEROW. Of course. They have a very extensive due process hearing in all the State jurisdictions.

I would point out that that would be the exception in terms of findings in that kind of an audit. The more common would be the fact that you might have a beneficiary going to a number of different physicians looking for controlled substances. In that case no individual physician would be aware of the other drugs being prescribed on behalf of that beneficiary.

So in most cases it is not the physician. It is the fact that the system is not alerting the beneficiary or the system permits the beneficiary to go shopping for controlled substances.

Senator COHEN. The Deficit Reduction Act of 1984 requires States to use tax data to perform client eligibility verification checks on applicants. Is this the trend? Your OMB guidelines, however, do not cover these up-front verifications?

Mr. WRIGHT. That is right, Mr. Chairman. We don't cover the upfront verification within the guidelines itself.

Senator COHEN. Isn't that the trend of the future? Everybody is going to start demanding that we verify eligibility of an individual by keying into Washington and various agencies as to whether that person would be eligible for benefits?

If that is the trend of the future, aren't you setting up some sort of a national data bank, even though it is not in one central office? You have several agencies; all the agencies have their own eligibility requirements. You thereby enable one State employee with a computer terminal to simply key into any one of those data banks, and they have got, in effect, a computer match without any of the protection that you recommend for the computer match itself?

Mr. WRIGHT. Mr. Chairman, first of all, you are asking a question that doesn't have a real easy answer, so let me try to summarize it.

I think we are going toward more front-end data verification, particularly in many of the entitlement programs, and that is the easiest way to reduce the error rates because once you get that data or false data into a computer you have to go through a much more extensive exercise to clean it up and then you have to actually take somebody off the rolls and go through a much more difficult process.

So I think we are going into an era of more front-end verification, but then you have a due process established that has to be followed where if the person is to be denied any access to Government programs then they ought to have a chance to verify and to refute the data and be able to go ahead and challenge the resulting match.

We are not going toward—I would call it—any kind of a national data base for several reasons.

No. 1, the technology isn't there to have what would be known as a full-scale data base between all of our files. As much as we would like to say—and we have been working to try to make them compatible—most of that work has been in the administrative area. It really has not been within the program area, and the technology simply isn't there right now.

It would be prohibitively expensive, and I am not so sure what you would get for it, to try to build a fully compatible data base where you could just go and punch in a number and get all the information—for example, like I saw, and I guess it was the Washington Post Sunday article going through that entire process. I just don't believe the technology is there.

Second, programs are not managed and organized that way. Anybody who has worked within Washington for any period of time knows that it is very, very difficult to get these agencies to work together on the most basic computer matches or cooperative arrangements, and Dick Kusserow can state that more than I can. He has had the frustrations trying to work with that.

And also, the laws in many cases forbid us from sharing data; for example, section 6103 of the Tax Code.

And then, finally, this is an area, and properly so, that has a great deal of public oversight, not only from the Congress but from quite a few groups that you are going to be hearing from today that are watching this continually, and well they should.

So I don't believe we are going toward any kind of national data base, but I do believe we are going toward better matching on the front end to make sure that those people who are participating in the programs, at least at a minimum, have some type of screening.

Senator COHEN. But you wouldn't support extending these kinds of requirements to up-front verification?

Mr. WRIGHT. I think on the up-front verification you shouldn't. If you were going to deny anybody access to Federal programs that they could be eligible for, they ought to have a chance to refute that and they ought to have a chance to correct the record.

But in terms of doing any type of prenotification, no, Mr. Chairman, I do not believe that is workable.

No. 2, I think that would be prohibitive from a cost standpoint.

No. 3, I am not so sure you would want to do this in many cases.

Let me give you an example. The program which I believe we all support, where we are trying to find those fathers of children who have left without making child payments, I don't think we would want to try to notify them beforehand that we are trying to do a match to find out if any of them have an IRS refund.

Senator COHEN. I would agree with that. These types of law enforcement matches would not be covered.

Mr. Kusserow.

Mr. KUSSEROW. Yes, Mr. Chairman.

I would like to add that, first of all, we have looked across almost all the Federal programs, and I am not aware of a single program that doesn't have the one essential feature that we all agree should be there before any final determination is made, either on the front-end side or if they are already in the system and that is, final determination should not be made without the beneficiary having an opportunity to confront the evidence with a real live human being before any final answer is made.

I would also tell you that every Federal program that I am aware of has that built into the program. I am not aware of any abuse that has taken place in that regard. Almost all programs have an established system of due process which includes some way to get to a hearing officer or an administrative law judge to appeal the errors of a program official.

So I first would agree with you that it should exist everywhere. At the same time I think in the Federal programs it does already currently exist. We are doing a very careful search right now to see if there is any exception to that rule.

Senator COHEN. Let me give you an example. OTA is going to testify shortly that "there is no agency compliance with the computer matching guidelines. In effect, the guidelines could be ignored. OMB has adopted a passive role, as evidenced by its lack of information on the scope and magnitude of computer matching and the quality of the personal information used, and the results and cost-effectiveness of computer matching."

Additionally, the GAO is going to be testifying, indicating deficiencies in the agencies' interpretations and compliance with OMB's computer matching guidelines, and saying that OMB wasn't aware of the problem.

It is not as if problems don't exist. There may be some safeguards, but the point of OTA and GAO is that there are serious problems in the program.

Would you find any objection to what OTA and GAO has said?

Mr. WRIGHT. Mr. Chairman, I would never try to say that what we are doing is perfect, by any stretch of the imagination.

Mr. KUSSEROW. And I would like to say that I have never found OMB passive in any of their authorities that I have witnessed in the last 5½ years, Mr. Chairman.

Mr. WRIGHT. But I would say, Mr. Chairman—and I believe I have mentioned 20 matches—those have gone in the Federal Register, and while I will say that that is not exactly what you call a best seller——

Senator COHEN. Now, the bill requires actual notice, and I think you take exception to this in terms of the costs involved, and I appreciate that. But notice in the Federal Register is not enough. Other than the Congressional Record, the Federal Register is probably the least read document in this country.

Is it fair to say that somebody who is getting a social security check or an AFDC payment or a welfare mother is going to be checking the Federal Register to see whether her records are being matched?

Mr. WRIGHT. No, sir. The point I was making is we have been noticing it. No question about it, the Federal Register is not a best seller. If you have ever read it, you will understand why.

But the people, for example, who will be testifying today I am sure do read it very carefully, particularly in the area we are talking about right now, and to date we have not received any concern about any of those 20 matches that I am aware of, whether there were any major problems, any serious difficulties, whether or not the Privacy Act was violated.

As I mentioned in my testimony, this is not because of the fact that it just comes into OMB. It is just because of the fact that there has been a great deal of time and effort between OMB and the agencies beforehand to make sure that those do comply with the Privacy Act.

Again, that does not mean it is perfect, by no stretch of the imagination, but you do have a process in there where you do have organizations reading that Federal Register very carefully to make sure that they are on top of whatever is going on within this area, and I think that is a very good notification process for many individuals.

To actually prenotify in many of these cases, I think you would literally bring the matching process to a halt, and in some cases all you are doing is prenotifying. The agency wouldn't be doing any of these things.

Senator COHEN. What about when people sign up for a particular program at the eligibility stage? What would be wrong with putting a notice saying that as part of this application you are hereby notified that your eligibility is going to be matched against tax records, against veterans' benefits, whatever else it might be that is in the hands of the Federal Government? Why can't that be done?

Mr. KUSSEROW. The problem would be that if that was a condition, prior to any match that every individual had to be notified, of course it would not always be possible.

For example, as you point out in the absent father program, if you are going to use their income tax returns to make sure they are not going to get refunds when their families are suffering, the problem is that the absent fathers are absent. We don't know where they are located. So how do you notify them?

Senator COHEN. We are talking about people applying for food stamps, for some other type of assistance.

Mr. KUSSEROW. What about the people that are already on that haven't had that notification?

Senator COHEN. When you mail out the check, for example, why don't you have a preprinted card?

I get them in the mail all the time. A preprinted card goes in along with the check saying, by the way, you are subject to having your records matched by the Federal Government.

Mr. KUSSEROW. There you have the difficulty—for example, let's take Social Security. We have about 35 million checks that go out each month in Social Security, but we have about 200 million active files. For 35 million, we know where they are because we are mailing checks to them. For the others we don't know where they are. How do you notify those individuals?

Mr. WRIGHT. What you are saying, Mr. Chairman, though, is some kind of notification that says you may be. You are not saying you will be; you are saying may be.

Mr. KUSSEROW. You are saying a one-time alert to somebody when they come on a program?

Senator COHEN. And a periodic alert.

Mr. KUSSEROW. If we could work out a system to do that and still not preclude the possibility of looking at or trying to determine matching against the other Social Security numbers of people who are not beneficiaries, if we can work out the mechanics of something like that, I think that notice would be fine. If we were to do it every time you wanted to do a match in Social Security alone, the additional cost of mailing would be something like $6 million just for the 35 million beneficiaries, not counting the labor for mail stuffers.

Senator COHEN. I think we are sensitive to that. We are trying to find some form of compromise between the actual notice each and every time there is a match and alerting them that their records—as part of participating in the program, in fact—will be subject to this type of periodic matching.

Mr. WRIGHT. Mr. Chairman, we will be glad to work with you on that. I think what you are saying is just some type of notification that makes sure that they are aware that they may be matched, but it does not force us into a match every single time.

In some ways I kind of like that idea because I think prevention on the front end, if you can get people to act right on the front end before you even have to go through the entire process, that is probably the most efficient way of doing it.

Mr. KUSSEROW. And that would not be entirely novel. In most of your benefit programs when you apply for a benefit, there are notices relating to the fact that there would be verification of information and things like that. So it is not as if you are starting out with no precedent whatsoever.

What you might be able to do is clarify more specifically what that means.

Senator COHEN. In your testimony, you said OMB should have the authority to waive publication for matching notices in the Federal Register if the agency could demonstrate public harm that would result from delaying the match.

Could you give me an example of what you mean?

Mr. WRIGHT. The key thing here is we are talking about in the law enforcement or when we are——

Senator COHEN. We are excluding law enforcement. We are not trying to cover that.

Mr. WRIGHT. Well, another example would be in Medicare and Medicaid where the doctors are going to do any double billing, and if we announce beforehand we are going to do the match, it is a very simple thing. They would just stop double billing.

Mr. KUSSEROW. An example of that, Mr. Chairman, might be when we periodically test emergency transportation services' billings for ambulances. The best way to do the match to test for abuse is to go on the assumption that if somebody were to be picked up and transported for an emergency medical reason then they should show up in a hospital somewhere, either for inpatient or outpatient services.

So we periodically check to see whether the ambulance companies are trying to bill for routine services such as going to a renal dialysis facility or a routine doctor visit. If you announced in advance that you are going to do something like that, they would stop doing it during that period of time, and they do it again later.

So we would like to do those kind of unannounced to find if there are abuses.

Senator COHEN. Would guidelines be issued so that simply "loss to the government" would not allow you to waive the notice requirements?

If you just adopt a broad policy saying that we are going to waive notice requirements here because the government is losing money, that is a wide door that is open.

Mr. KUSSEROW. It is not so much that we are losing money; it is why this abuse takes place and how can we limit this vulnerability in the future. It is not so much the dollars as trying to get the program to work efficiently.

Senator COHEN. What I want to know is what guidelines would you use to allow you to invoke the waiver. What is the standard you are going to use?

Mr. WRIGHT. Mr. Chairman, we will be happy to work with you on that.

I think the question you might be asking is would we open up a very wide waiver, and the answer to that is, no, not at all.

Senator COHEN. How would I know that, though?

Mr. WRIGHT. We would be more than happy to go ahead and work with your staff on that.

Senator COHEN. You say that you would support minimum due process requirements in order to avoid confusion among the agencies.

What sort of minimum protections do you envision—notice, verification, opportunity to refute information?

Mr. WRIGHT. Yes, sir. I believe, as Mr. Kusserow said, that at the present time there is a due process procedure within all the agencies, and I believe if there are any problems I would like to know what they are so we could go ahead and correct them right now before any legislation might pass.

But as far as I know, those procedures are carried out basically by the agencies. If they are not, we will be more than happy to go and make sure they are.

I don't see any major changes there, but there certainly would be notification. Certainly there would be a chance to refute the information and be able to go through, if need be, back through administrative legal proceedings.

Senator COHEN. Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you, Mr. Chairman.

First, I have a brief opening statement.

Senator COHEN. You can waive that. [Laughter.]

Senator LEVIN. The part I don't want to waive is my commendation to the Chair.

Senator COHEN. Take as long as you like. [Laughter.]

Senator LEVIN. That was just the first paragraph, but we will expand that paragraph for the record.

I do want to commend you, Senator Cohen, for what you are doing in this area. It is a very critical area.

You are balancing a lot of important interests that you have brought here, today. I commend your talents and your devotion to balancing the needs of individuals for privacy and due process with the needs of government to be protected against fraud. They are very unique talents to bear on this issue. The result is the bill that you introduced and which is the subject of this hearing.

And the balance of my statement I would like placed in the record.

[Senator Levin's prepared statement follows:]

PREPARED STATEMENT OF SENATOR LEVIN

I commend my friend, Senator Cohen, for holding this hearing and once again addressing the important issue of computer matching.

Computer matching is a powerful new tool of the modern age, and it is obviously here to stay. Computer matching increases the efficiency of Government operations and helps identify persons who would defraud the taxpayer by taking unearned benefits from Government programs.

Like other powerful tools, however, computer matching is dangerous when misused and it is capable of being abused. It can run roughshod over the privacy concerns of individuals and, through old or inaccurate data, result in the erroneous termination of Government benefits. To stop computer matching activities from unfairly steamrollering individuals in our society, safeguards must be developed and implemented.

The problem we have to deal with is the complex computer program which is designed to help Government officials run their programs fairly and efficiently but which ends up hurting individuals—reducing the disability check of a handicapped individual who will have a hard time protesting the action or cutting off the pension check of an elderly American who can't survive the amount of time it takes to convince the authorites that the computer is wrong. We have to prevent the creation of a computer program like the one in the motion picture, "2001," which means well but hurts the individuals it is designed to help.

S. 2756 provides some of the safeguards we need to control the use of computer matching. It requires agencies to enter into written agreements governing the collection and use of computer matching data and requires them to set up internal boards to monitor computer matching activities. It also provides individuals with notice that their records are subject to computer matching and, perhaps most important of all, requires agencies to independently verify all computer matching data before reducing, suspending or terminating an individual's benefits. This safeguard is necessary in light of the extremely high error rates found in computer matching data.

With controls, computers are enormously helpful tools; without them, computers can play havoc with our lives. S. 2756 is one effort to implement reasonable controls on computer matching, and I look forward to hearing what our witnesses have to say about its provisions.

Senator LEVIN. I have a few questions of Mr. Wright, first on the question of what studies have been made by Federal agencies—of the efforts that they have made.

I understand that in Massachusetts there is a project which recently matched bank records to identify individuals with assets that were above a welfare program guideline and officials were able to verify that only 6 percent of the raw hits produced by the computer match. In other words, 94 percent of the people who were identified in that match as having excess assets and who would have been disqualified from the receipt of those benefits were later found not to have excess assets.

Senator COHEN. The number is something like 6,482 raw hits and 384 cases of abuse out of the 6,480.

Senator LEVIN. All those persons would have had their benefits terminated if Massachusetts did not require independent verification of all information produced by computer matching programs.

Do we have any statistics on the experience of Federal agencies regarding what percentage of the raw hits from a computer match are eventually verified as being correct?

We have the Massachusetts example—that project—you say that Federal agencies are now doing this verification and, as a matter of fact, you recommend independent verification. I understand from the testimony that you do support independent verification when there is a computer match.

So we have had experience in Federal agencies. What is the experience?

Mr. WRIGHT. OK. Senator, I don't have the experience right here with me. We have done 20 matches, I mentioned to the chairman, and we do have the experience on those 20 matches. We can give you the data—correct me if I am wrong, Dick—on those 20 matches and what the raw hits were and what resulted from the matches—in other words, the number of dollars that were spent.

Senator LEVIN. What I am interested in is the number of raw hits in each match, then how many were verified.

Do you have that information?

Mr. KUSSEROW. Senator, that would vary on each match. I think the important ingredient in that is that no action is taken to the detriment of anyone until those raw hits are refined by further review or investigation by live human beings, and in that case we can give you three things.

We can give you the matches we have done. We can give you the raw hits, and then from the raw hits what the final result was.

Senator LEVIN. I am interested in a statistic between two and three. I am interested in what percentage of the raw hits were independently verified as well as what the outcome was in terms of dollars.

Mr. KUSSEROW. We can give you that.

Senator LEVIN. If you could supply that for the record.

You don't have any material available to you today?

Mr. KUSSEROW. I can cite you an example off the top of my head if you would like. A couple of years ago we looked at the Medicare termination notices due to death.

Now, in America today it is pretty hard to die without the doctor putting in a final bill. In the case of Medicare they have a form they fill out, and it basically will show that the operation was successful, unfortunately the patient died and this is my final bill.

We bumped the Medicare termination notices due to death against the master beneficiary record of Social Security. This is basically the same population, the same 35 million people. We came out with 8,500 people who were declared dead by Medicare and who were still being paid Social Security benefits.

Now, in looking at that, we did not take action on that 8,500 because we really didn't know what that meant yet. All we know was that there was discrepancy.

Senator COHEN. Are they in Chicago? [Laughter.]

Mr. KUSSEROW. A good portion of them are.

So the next step would be to try to understand the data.

What we subsequently found out, Senator, was that about 2,500 of them were still alive. The reason that we found them in the data base as dead was that on the Medicare notice adjacent to the line for the fact that the patient died was the line for the fact that the patient was discharged. Physicians got a little sloppy about where they put the mark, and so they made a lot of mistakes.

I can tell you that no action was taken against anyone until we had a positive verification in each case that they were dead, and that was a death certificate. Those we were able to cull from the record, and there was no action taken without that death certificate.

Senator LEVIN. You are able to tell us that out of 8,500 what number led to the termination of Social Security benefits?

Mr. KUSSEROW. About 5,500 of them were verified as being dead by death certificate.

Senator LEVIN. For those 5,500, in all of those cases were Social Security benefits still being paid?

Mr. KUSSEROW. Yes, sir.

Senator LEVIN. So there you had a better than 50 percent independently verified number?

Mr. KUSSEROW. We independently verify everything before we take action.

Senator LEVIN. I know that, but it turned out that the match was right in more than half the cases?

Mr. KUSSEROW. Yes, sir.

Senator LEVIN. Is it true that the raw hits usually contain a high percentage of errors?

Mr. KUSSEROW. Yes, sir, that is correct.

Senator LEVIN. That is what you will be giving us for the record?

Mr. WRIGHT. Senator, we will be happy to provide that.[1]

Mr. WRIGHT. I might also add that the Massachusetts example which we used is one that we have also talked a great deal about. It is an example of one where the procedures that we had in place were not carried out and there were no Federal agencies involved.

Senator LEVIN. I know. That is why I asked you about Federal agencies, as a matter of fact. We have the Massachusetts example, but we don't have a similar analysis for Federal agencies using computer matching, and I asked if you could provide that for the record.

Mr. KUSSEROW. We can give you that, Senator.

But I would also point out that that is why we have been trying to move toward up-front verification. One of the reasons why the hits are so inaccurate is that the initial data collection that was done at the program level was fairly sloppily done, and so it created problems.

We talked about Medicare termination notices and the sloppiness that created the mistake. So we find the best thing to do is on the front-end side, before somebody gets into the system; before somebody has bad data in their benefits file; before they get into the system, to do it accurately so the record is not full of inaccurate data.

Senator LEVIN. Mr. Wright, I understand that OMB supports making the independent verification requirement a part of every agency's procedure, making it a minimum necessary requirement in deciding whether to terminate a person's benefit, is that correct?

---

[1] See letter p. 234. Additional information will be retained in subcommittee files.

Mr. WRIGHT. Yes, sir.

Senator LEVIN. How many agencies are now doing that? How many agencies that are now doing computer matching have that independent verification standard?

Mr. KUSSEROW. All Federal programs we are aware of have that set of requirements, with due process attached.

Mr. WRIGHT. I am not aware of one, Senator, that does not have that requirement.

Senator COHEN. Is it a requirement, or is it only a suggestion that it should do this?

Mr. KUSSEROW. Departmental regulations most often govern that.

Senator COHEN. Is it mandatory?

Mr. KUSSEROW. It is mandatory. We have a very elaborate system of due process—various agencies with hearing officers, administrative law judges on the staff to provide independent due process in situations where the beneficiary wants to make a claim against a program.

Senator COHEN. That word "should"—we should interpret as being "shall"?

Mr. KUSSEROW. Yes.

Senator LEVIN. The OMB guideline, which I take it then you have no objection to being made into law, now covers matches that are done for fraud purposes, but I understand it does not cover matches that are done to determine whether or not a person is eligible to get benefits—the front-end eligibility verification.

Are you considering expanding your guidelines to cover those matches of front-end eligibility verification?

Mr. WRIGHT. Not at this time, sir. We don't really see a reason for it at the present time, either to cover the front-end verification or to cover the administrative matches that are quite often done.

Senator LEVIN. Why is that?

Mr. WRIGHT. Because we think if we are going to be sending out any guidelines there ought to be a reason for it. At the present time we don't see any major violations that are occurring.

We made it very clear to the agencies that whether it be front end or whether it be after the fact, that due process and independent verification before any action is taken to the individual should be conducted and to our satisfaction. That is being done.

Mr. KUSSEROW. If I may add, Senator, the most recent expression of the Congress on matching is in the Deficit Reduction Act of 1984. The inspector general community as well as OMB supported those features in that legislation with the front-end verification that would include the due process elements that were felt essential. We supported that and advocated it, including making sure that before any benefits are denied that a person has an opportunity to confront the program officials in person with their own evidence.

Senator COHEN. As I recall, we added that on the floor. I don't recall the administration putting that in. I think Senator Heinz and myself added that to the program.

Mr. KUSSEROW. The IG community went ahead and endorsed that and supported that because we felt that was appropriate to assure that everybody has a right to provide their own evidence that would be counter to that of the agency.

Senator LEVIN. Just one last question. What is the OMB's position on the bill's provision to place data integrity boards within each agency?

Mr. WRIGHT. Senator, we don't believe the data integrity boards are really necessary, and I would add probably—maybe the word "inappropriate" is too strong, and I am trying to get somewhere between "unnecessary" and "inappropriate"—level of committees and bureaucracies, and certainly everybody knows we have got enough of those now.

Senator COHEN. What is your administrative option?

Mr. WRIGHT. What we have got right now—oh, and one more problem I have as Chairman of the PCIE, the data integrity boards were proposed and my understanding would be separate from the inspector general, and the inspector general provides under the 1978 act a very important level of independence that reports both to the President and to Congress. I think we want to maintain that independence, and the data integrity boards could be interpreted as kind of infringing on that a bit.

But more importantly, I think that when the Financial Managers—pardon me—the Federal Managers Financial Integrity Act was passed, it provided an extremely important vehicle for assessing the vulnerability of agencies to not only fraud or financial mismanagement but also to inappropriate violations of the Privacy Act. There is no way out of it.

And several months ago I sent out guidelines to the agencies to place a high priority on the Privacy Act, computer matching and all the rest of it, in this year's report that is coming up to Congress.

Now, we have that covered under what we call circular A-130 from OMB. What I would propose doing is beefing up that circular to make sure that the concerns the committee has, as well as the administration, are properly covered, that we combine aspects of our circular A-130, which is the computer security and privacy guidelines we have been talking about, and have natural reporting mechanisms with the agency heads as a personal sign that this is the status within the agency of the vulnerability to anything, from the financial controls all the way to computer matching to the Privacy Act, to the Congress and the President, and it is covered also by the inspector general.

And that is what we would propose.

Senator LEVIN. Have you read the Office of Technology Assessment's report, which indicates a lack of oversight now in the agencies—are you familiar with that report?

Mr. WRIGHT. I am familiar with it, Senator. I did not read it, but I have been briefed on it.

Senator LEVIN. Thank you.

Senator COHEN. Just one other point with respect to other agencies. The GAO report that came out just last month concluded that the agencies need better coordination on the issue of privacy functions. Let me quote a portion of that report:

> The pervasiveness of shortcomings leads us to conclude that the Privacy Act operations need a cohesive, articulated program aimed at ensuring that such activities are conducted with full compliance with OMB guidance and the act's provisions. Without more active involvement and monitoring by both OMB and the agencies, there will be less than full assurance that the Privacy Act could be carried out in a manner that protects the privacy rights of individuals and balances the rights with the independent needs of the agencies.

So even the GAO is saying that those people within the agencies themselves who are involved in protecting individual rights under the Privacy Act are spread widely or pervasively throughout the administration at low levels and are not given much of a voice in formulating policy.

The purpose behind setting up a data integrity board was to establish a level high enough and to establish a comprehensive set of guidelines to make sure that these rights are being protected. As it is now, persons watching the Privacy Act are all diffused throughout the bureaucracy at very low levels, with these individuals also being required to take into account the need for efficiency, as well as protecting privacy rights.

Mr. WRIGHT. Again, Mr. Chairman, like I mentioned, in the overall bill we kind of agree with what your goal and objective is. I would say that it would follow the process that we propose. Of course, it could be some hybrid of that, and we could work together on that.

No. 1, the agency, the person in the agency who would be responsible for this would be the agency head because by law they have to personally sign these reports when they report to the Congress and the President. Then you have got the IG oversight and the Assistant Secretary for Administration who is responsible for preparing this. That is a pretty high level in these agencies. It is about as high as you can get.

The key thing is for us to go——

Senator COHEN. If that is the case, why is the GAO saying it is not working as it should?

Mr. WRIGHT. Well, GAO, you know, I love them like brothers, but that doesn't mean that in all cases that OMB and GAO agree. We have the responsibility of carrying out many of these acts, and they, rightfully so, have the responsibility of critiquing what we do, and I can't imagine they would always say we are doing a terrific job.

Mr. KUSSEROW. But the direct linkage between your concern and the Federal Managers Financial Integrity Act and OMB circular A-123 is not currently present.

I think he was saying that you could probably reach your same objective if OMB would revise the circular to focus on the privacy and protection aspects of data integrity and then make the agency head sign off on it.

Now, in our department that would be the Secretary. The data integrity boards from the inspector general's viewpoint cause a little bit of concern.

The reason is that when we are auditing a program, and find errors in the program, it reflects adversely on the program manager. So if the program manager were on the data integrity board, you would find that they would not want the inspector general mucking around with their turf.

So if you raise it high enough—that is, to the agency head—then you would get away from those little turf issues that exist within agencies, where people are afraid to have their programs be disclosed as inefficient or error prone.

Mr. **Wright**. This would also be an established congressional report, which I think is a vehicle that is in place. The agencies I believe are coming in. It does have GAO and OMB views.

The only other thing I would say, Mr. Chairman, in response to the GAO, out of the 20 matches that we have had we have not received any major complaints or concerns about violations of the Privacy Act.

Senator **Cohen**. Thank you very much.

Senator **Levin**. Let me just ask one question. In terms of all the agencies who are doing computer matches, has there been any litigation on this issue that you know of—any lawsuits brought against any agencies based on some kind of abuse or inaccuracy or error?

Mr. **Kusserow**. None.

Senator **Cohen**. We look forward to working with you, Mr. Wright and Mr. Kusserow, toward a bill that will have your support.

Mr. **Kusserow**. We would be delighted to help.

Mr. **Wright**. Thank you very much.

Senator **Levin**. If possible.

Senator **Cohen**. If possible.

Senator **Levin**. You say you love the GAO like brothers—that threw some doubt on the rest of the testimony, I must say.

You don't have to comment on that.

Senator **Cohen**. I think it is a Cain and Abel type relationship. [Laughter.]

Thank you.

Our next witness is Joseph F. Delfico, Senior Associate Director of the Human Resources Division of the U.S. General Accounting Office.

Mr. Delfico, in view of the fact that we have discussed your testimony at length here, perhaps you can just summarize it for us.

TESTIMONY OF JOSEPH F. DELFICO, SENIOR ASSOCIATE DIRECTOR, HUMAN RESOURCES DIVISION, GENERAL ACCOUNTING OFFICE,[1] ACCOMPANIED BY DAVID PASQUARELLO, EVALUATOR (PHILADELPHIA OFFICE); RICHARD HALTER, ASSIGNMENT MANAGER (PHILADELPHIA REGION); AND DANIEL BRIER, GROUP DIRECTOR, HUMAN RESOURCES DIVISION

Mr. **Delfico**. Thank you, Mr. Chairman.

With me on the left is Mr. David Pasquarello and Mr. Richard Halter, who are responsible for the work we are doing for the committee, and Mr. Daniel Brier, on my right here, who is in charge of my welfare work.

With your permission, I would like to submit my full statement for the record and present a summary.

---

[1] See p. 77 for Mr. Delfico's prepared statement with attachment.

We are pleased to appear today to discuss the preliminary results of the work we are doing at your request on the Deficit Reduction Act of 1984 and provide our views on S. 2756, the Computer Matching and Privacy Protection Act of 1986.

The Deficit Reduction Act requires each State to have income and eligibility verification systems in place by October 1, 1986. Among other requirements, DEFRA requires State agencies responsible for the State and Federal welfare programs to use certain Federal tax information as a check on the accuracy of the income deferred by applicants and recipients. In addition to State administered programs, DEFRA authorizes the Supplementary Security Income Program, which is administered by the Social Security Administration, to access and use, for eligibility verification programs, unearned income data from the IRS.

Based on your 1985 request to monitor the implementation of DEFRA, we reviewed the Federal rules and comments on those rules, and we sent questionnaires to all State levels inquiring about the current status of implementation in each State. All but 4 of the 53 respondents said they expect to have their required systems and necessary staff in place by October 1, 1986.

One reported problem common to the 32 States is that current automated systems will be postponed or disrupted for periods of 9 months or longer, while those States divert resources to making reprogramming, procedural, and other changes to their existing systems to meet the October 1 deadlines. Most of these States reported that in the interim they would be operated less than fully efficient systems requiring caseworkers to do more manual case reviews.

A number of States expressed concerns to us about the need for clarification in interpreting and applying different rules. Many of their responses, for example, indicated concerns about the allowable time to process their caseloads.

One area in which nearly all States said they anticipated no problems is in the safeguarding of data. Data agencies administering the needs-based programs, regularly attain, use and safeguard personal data during the normal course of their work. Most States require that their existing systems insure the security and confidentiality of data. Thus, they anticipated no problems in meeting the standards established by IRS and the Social Security Administration for safeguarding their data.

Most States, however, expressed some concern about the costs to do the match, outweighing the predicted benefits.

Since State agencies administering programs under DEFRA have virtually no experience using interest and dividend tax data for eligibility verification purposes, we feel it is premature to reach conclusions about the States' initial predictions.

To our knowledge, the only comparable experience to date is the match of SSI recipients with interest and dividend data. This match showed substantial net savings. Without this tax data, such results could not have been realized. Now this was a match performed by the Social Security Administration. However, more accurate estimates of cost and benefits, we feel, will become available after the States begin to use tax data, at which time they will be in a better position to make assessments.

More detailed results of our survey are included in the attachment that I submitted for the record.

I would like to briefly go over in the remainder of our statement our comments and views on S. 2756.

First, you asked our views on the type of matches that should be covered by the bill. We believe a distinction should be made between computer matching to verify eligibility in Federal payment systems and matching done for such other programs as law enforcement. In either case, the flow and usage of data for matching needs to be controlled to protect the privacy of individuals.

However, criminal investigations or similar Government activities outside of benefit payment system management might be adversely affected by certain bill provisions. Section 2 requires an agreement to notify individuals and section 3 requires advanced Federal Register notification about upcoming matches. Such notifications could neutralize the effects of law enforcement matches which, by their very nature, must be kept confidential. But we are also concerned that law enforcement agencies properly protect information and guard against unwarranted disclosure or abuse of information they gather. To that end, we believe such agencies should have data integrity boards to oversee these functions.

We support extending the bill's provision requiring matching agreements to State agencies administering federally financed benefit systems. We take this position because these agencies, in essence, manage Federal programs and have legitimate informational needs to verify declarations made by applicants and recipients.

You asked us to comment about matching agreements required by section 2 of the bill. Basically, we believe that this section is fairly complete. It provides information for future audits and established a much-needed vehicle for review and oversight of data. However, some clarification and redefinition would be helpful. The bill is unclear with respect to the scope of the matching agreements. If your intent is to make all matches, including those disclosed under subsection (b) of the Privacy Act, subject to matching agreements, then you may wish to make section 2 a separate section of the Privacy Act rather than including it as another of the act's disclosure conditions.

Second, you may wish to consider the need for matching agreements to be tailored and adapted to the particular needs of certain agencies such as law enforcement agencies discussed earlier.

Third, we question why there is a requirement after the agreement is reached between agencies for 30 days to elapse before data be disclosed. In some cases and in some matches, timing is important, because of the relatively rapid movements of recipients on and off the rolls.

Section 2(d), dealing with notifying individuals and matching programs should, we believe, specify the method of notification to be used, particularly those that involve large data bases. Our statement for the record contains some suggested language dealing with this issue.

Senator COHEN. Mr. Wright testified about the need to waive requirements under some circumstances. Do you address that?

Mr. DELFICO. Yes. With regard to law enforcement agencies, we have addressed whether certain provisions should apply.

Senator COHEN. Not even law enforcement. What about the double billing of doctors under Medicaid and starting to notify them that they are going to be checked and matched, and they stop double billing or the ambulance that is not performing routine services that Mr. Kusserow talked about. Are those legitimate cases in which there should be a waiver of notification?

Mr. DELFICO. I see these matches in the same category as matches of welfare program recipients. I think if we publish the fact that we will be verifying their eligibility for payments, it may help the programs. Particularly, it may help screen abusers from the programs.

Senator COHEN. I am talking about checking the doctors now. You know that under Medicaid you've got some doctors who are double dipping, and they want to match up those records of that particular doctor and that particular patient, in terms of what's been going on.

Should there be a notice of waiver under those circumstances?

Mr. DELFICO. I think circumstances such as those deserve special consideration; yes.

Senator COHEN. So in those cases in which there is a likelihood that the activity, the ongoing activity could be terminated by such a notice, do you think that some sort of either internal regulation or some sort of guideline ought to be established, whereby we could determine whether it is a proper waiver, as opposed to simply saying, whenever the Government is going to lose money, we can waive the notice requirement?

There has to be some sort of guideline, either internal or external, whereby this committee and others can judge whether there's been an abuse of a waiver.

Mr. DELFICO. One way to handle that would be through the matching agreements by spelling out, in the matching agreements, what the considerations need to be to cause a waiver of notice.

Senator COHEN. I am sorry I interrupted your presentation.

Mr. DELFICO. We suggest, finally, and this is going back to section 2, the addition of a matching agreement provisions specifying that feedback be also provided to the source agencies on the accuracy and completeness of its records. This will assist the source agency in correcting any inaccurate or incomplete data in its data base.

I think if the bill requires that the source agency receive such information after matches from the matching agency, it will learn a lot about the data base. And this will help clean up its data base.

Senator COHEN. What was the experience of the State agency, in terms of getting data from the IRS and Social Security Administration, How old was the data they were receiving?

Mr. DELFICO. When they begin requesting data next month, they expect the data to be between a year and 2 years old.

Senator COHEN. Is that reliable information on which to determine the benefits?

Mr. DELFICO. In some cases people were and are still on the rolls. So if the States have payment data that goes back 2 years for a particular welfare program, they may find it to be reliable. But we found that the States do not keep historical data, so it could be an expensive proposition at the start to develop their files to match someone's income with the year and a half to 2-year-old data that they receive from SSA and IRS. It should be a temporary situation, however, until the States start building up their records. But one of the items that the States addressed for us on the questionnaires was the age usefulness of the Federal data.

Senator COHEN. If they have information 2 years old, given today's volatility in the economy, it would seem to me that would not be adequate verification in approval or disapproval of benefits.

It only heightens the need for verification of the information, initially. That will save money in the long run, and make possible more good managment of data. Ultimately, it will save the agency money.

Mr. DELFICO. I believe you have clearly emphasized the need for verification in section 5 of the bill.

Senator COHEN. One final point. What about the data integrity boards? You heard Mr. Wright indicate, that we should not put another level of bureaucracy in an already bureaucratic system. We don't need them. We propose in circular A-123 that we can upgrade the quality of review and intergrate questions about privacy protections and the need for efficiency without putting a data integrity board into the process. What do you think?

Mr. DELFICO. We feel that data integrity boards are needed with a minor qualification, and that is, their size should be tailored to the activity of the particular agency that they represent.

For example, a data integrity board at the Social Security Administration could be quite large, compared to one for the Railroad Retirement Board, which is a small agency. We see the need for data integrity boards, because we have found that there is a general deemphasis of privacy offices in many agencies.

If we could somehow couple the data integrity boards with the privacy officer structure, it may help ensure compliance with some of the requirements in the bill.

Senator COHEN. What about the argument that you might be treading on the independent toes of the inspector general, which is inconsistent with existing practice?

Mr. DELFICO. I think if you raised the data integrity boards to a high enough level within agencies, it will help avoid that situation.

Senator LEVIN. Would you have the inspector general to serve on the board?

Mr. DELFICO. That is a consideration. I haven't thought that one through, but as Mr. Wright was speaking here earlier, I thought that it is an option, yes.

Senator LEVIN. I was interested in your position on the data integrity boards, too. Would you give us, for the record, something on the makeup of those boards if you think that the legislation ought to suggest, or require certain people, such as the IG, to be on the board? Could we have a recommendation on that, for the record?

Mr. DELFICO. We could work with the committee on that. We've done some thinking on it but we are not firm yet. We think the board should be sized to the agency and the amount of the activity that the agency has. We will consider whether the inspector general should be part of the board. Boards should be at a high enough level, but in some agencies like HHS, there are a number of subagencies that are often large. We are not clear yet on how those agencies could network for board purposes.

For example, the Social Security Administration probably is the largest of the agencies within HHS, and it would probably need a large board or large staff to handle the data integrity board issues. So we haven't completely worked that out, Senator.

Senator **Levin**. Mr. Wright said, as far as he knows, all agencies are now verifying independently the data which is produced by these matches. That is a little different from my understanding. Is that your understanding, as well?

Mr. **Delfico**. My understanding is that they are getting better at verifying than they were in the past. I think there is more focus on the privacy issues.

Senator **Levin**. Do you know that all agencies, in fact, now independently verify that data?

Mr. **Delfico**. I can't support that. We don't know.

Senator **Cohen**. Didn't you also indicate that there were insufficient guidelines? That there is little in the way of oversight? OMB was passive?

Mr. **Delfico**. Yes; we did.

Senator **Cohen**. Wasn't that a little inconsistent with what you were saying?

Mr. **Delfico**. I said they are getting better. I didn't say that they are where we would like to see them. Our recent report did note that there are quite a few shortcomings in the way they are administering the Privacy Act. In the report we make a number of recommendations to OMB.

Senator **Levin**. As I understand your position from your previous statement and testimony, with whatever qualifications you've given or explanations you've given, GAO supports the bill?

Mr. **Delfico**. Yes; we do.

Senator **Levin**. One other question on the OMB guidelines. Until this bill is passed, should the OMB extend its guidelines to front-end eligibility verification?

Mr. **Delfico**. Yes; I think that would be good. I think right now, as the testimony was being given, that there is a loophole there.

Senator **Levin**. Thank you, Mr. Chairman.

Senator **Cohen**. Thanks very much for coming this morning, Mr. Delfico. We will include your testimony in full in the record. It will be very helpful to us in trying to fashion the bill itself.

Next we are going to hear from Ron Plesser, representing the American Bar Association. I would point out that Mr. Plesser has served as general counsel of the Privacy Protection Study Commission and has testified before this subcommittee in the past.

TESTIMONY OF RONALD L. PLESSER, AMERICAN BAR ASSOCIATION[1]

Mr. **Plesser**. It's good to be back with a somewhat different hat on this time. Senator Cohen, Senator Levin, my name is Ronald Plesser. I'm pleased to accept your invitation to testify at these hearings as the official designee of the American Bar Association president, Eugene Thomas.

---

[1] See p. 92 for Mr. Plesser's prepared statement.

It is with unique pleasure that I come to this subcommittee to strongly support your efforts to enact legislation to establish safeguards for computer-matching programs.

I'm a member of the governing council of the individual rights and responsibilities section of the ABA. I was general counsel for the U.S. Privacy Protection Study Commission, and I've spent many years working with the Privacy Act.

The views I express today are the views of the American Bar Association, based on the resolution supporting this legislation which was adopted at its annual meeting during August of this year in New York.

Before I go into detail in terms of the ABA recommendations and our strong support of S. 2756, I'd like to put on the record a little history in order to provide you with some appreciation of the ABA process.

My sitting here today saying that I represent the president of the American Bar Association is not just a simple fact. It took a lot of effort. It took many years of coordination of various ABA entities.

So I think that the recommendations that we present today are not just several people sitting down in the Government Affairs Office deciding that this is a good idea. These are recommendations that have been supported by the ABA's full policymaking House of Delegates. There has been very strong participation in the individual rights section, the section of science and technology, and many other sections of the American Bar Association.

In summary, the policy of the ABA is fully consistent with the provisions of S. 2756. There are, in addition, several provisions in S. 2756 which were not considered by the ABA and, thus, on which we have no position.

We will be consulting with the section of science and technology and other interested ABA groups on these provisions. However, I am here today to express the very strong support of the American Bar Association for S. 2756.

The bar association, before we went through the process of getting approval of our recommendations, met with government officials, people from your staff, people from the staffs in the House, from Mr. Kusserow's office, the Office of OMB. We've done that for 2 years. And we've sat down with all the interested parties and we've tried to come up with a set of recommendations and policy approaches which we think resolve the current problems.

We think that the recommendations we've come up with, which by and large are reflected in your legislation, resolve most of the problems in the matching area. I'd like to just mention several of the differences perhaps between the ABA's recommendations and your legislation, and to suggest strongly that our recommendations be considered.

The first is that our recommendations are not limited to government to government, Federal to Federal or Federal to State actions. They cover private sector matches as well.

We believe this is a very strong, very important distinction. I think, as we heard this morning from Mr. Kusserow, there are matches going on with private doctors under Medicaid. And I think that kind of situation should be as regulated as any match with a State government.

Let me say as a footnote I was amazed at the conversation because Mr. Kusserow seemed disappointed that the notification procedures resulted in the doctors not over billing. Without having to spend any time with enforcement personnel or trials, or administrative decertifications, they seemed to have obtained compliance simply by putting a letter in the mail. If the result of notification of a match would be to stop all double-billing on Medicaid, I think that would be an absolutely fabulous result and the best justification for notification I've ever heard.

They seemed disappointed that the doctors stopped doing it so that they couldn't prosecute the ABA's recommendations, need to be considered in terms of continuing into the private sector, as well as the Government.

Senator COHEN. Could I stop you there? You think there should be no waiver of notice under any circumstance?

Mr. PLESSER. Of notification? I really don't see any reason for a waiver under any circumstance. To my understanding, matching programs are primarily audit tools developed by the inspector generals to assure that the agencies are doing a good job.

It's really an administrative check. It's the way they investigate their own agencies. In some cases, of course, it has this effect of picking up people who have worked through the system.

I can see absolutely no reason why there shouldn't be notification of a matching program. Every agency has to publish in the Federal Register a system of records notices for Privacy Act purposes. They can't collect information without those notices.

I really don't see in this circumstance why a 30-day notice of a matching program would in any way jeopardize legitimate administrative activities.

Senator COHEN. So, in this particular case, if they were going to conduct a match to check an outfit they might suspect is engaged in overbilling or a series of doctors who are engaged in overbilling, if they put out a notice regarding the match, you regard this as a deterrent against them continuing that process?

Then they go back and match the records and find out he has engaged in double-billing and turn it over to the attorney general? Is that what you're saying?

Mr. PLESSER. I would have no problem with that. I would think the notification restrictions probably are far more general than telling him to notify the particular doctor that his particular records—his or her particular records—are going to be matched.

I think we are really talking about system and usage notices. If you're going to take a doctor's privileges away, then you have to give him specific notice that a match has been made.

But, again, I think, as Mr. Kusserow said, most of the Government benefit programs already have a hearing and other due process. If somebody's Social Security rights are removed, you have a right to some kind of fair hearing.

The other difference between S. 2756 and the ABA recommendations is that the ABA recommends substantive restrictions as well as the procedural rules set up in S. 2756.

The first recommendation of the ABA states that the Privacy Act of 1974 should be amended to prohibit nonconsentual use of income tax, census, political activity, religuous affiliation and similarly sensitive data files for the purpose of verifying the eligibility of citizens for Government benefit programs.

I think the approach of S. 2756 is quite excellent in its provisions leaving those questions to the data integrity board. But it's the ABA's position that the legislation itself should have some substantive standards for those types of information, that perhaps it would take something like an act of Congress, like was done recently in the Debt Collection Act, to justify the use of IRS or other kinds of material.

I would hate to think that Government administrators would have the ability to match tax, census, political activities, or religious affiliations without a specific mandate from Congress.

Now, the Privacy Act in section E-6, of course, has some limitations on the use or collection of some of that type of material. But, really, the limitation is only to the extent the information is authorized to be collected. While it's an effective limitation, I don't think it's enough.

Let me say that I think the bill as it stands, primarily as a procedural bill, is excellent, and I certainly agree with the other witnesses who have testified today that the procedural protections are an important step forward.

We would just like to suggest that a look at the substantive standards also be made to see if there is any possibility of adding such standard.

A connected question is the routine use or incompatible purpose test that's in the Privacy Act and it's not specifically mentioned, of course, in your legislation.

I've testified before this committee about how I think that that routine use provision is so big an exception that you could drive a truck through it. That still holds, although I think the concept is still a good one.

It's the enforcement of that that's been disappointing. I would think that either legislative history indicating that you intended the compatibility purposes test would apply, because this is being amended to the Privacy Act, or that there be some specific mention of it with a good deal of legislative history indicating that this committee really thinks that that phrase means something, that information is going to be collected for only one purpose.

I think that the role this committee can have is very significant in the development of that, not only for matching programs, but I think also for the Privacy Act generally.

We, of course, support specific notification. I think I agree with you that there can be some middle ground between writing a letter to everybody and general notification.

The Privacy Act itself, of course, which wasn't mentioned, requires notices not only in the Federal Register, but in your IRS statement, or in the benefit program statement if the Government is going to collect information on taxes. The form in which information has to be collected, must contain a Privacy Act statement.

It seems to me a matching statement could easily be included with those actual forms of the person who is filling out the material; when they are doing it, they would have the opportunity of being notified.

I think notification, as I mentioned before, is crucial because it is obviously the idea, I think, is not fraud and abuse, it's that fraud and abuse can be stopped because people know that this information is being used.

I think that's far more beneficial than letting them work into the system because they're not notified of it, and having to spend all the money for enforcement activities.

Senator COHEN. You've answered every question I have except one. What about sanctions?

Mr. PLESSER. I talked to Mary Gerwin on your staff the other day about it. I've always testified that I think the Privacy Act sanctions are not sufficient because of the impossibility of demonstrating damages. And I think that is really exacerbated in this case.

The reason why I think there's not a lot of abuses or reports of abuse is because it is so hard to identify, and it's so hard for people who are notified who don't know what's happening to their records.

I think proper notification would perhaps increase it. But I think that some strengthening of the Privacy Act penalty provision, of the liquidated damage provision, or some kind of provision that motivated an individual to make the effort to find out would be appropriate.

Again, that is not a position specifically mentioned by the ABA. So I defer to my previous testimony, that certainly that's not ABA, but I think that the provisions in your legislation in terms of saying that if someone who violates them, they cannot do further matches is actually very good.

But it's an all or nothing kind of situation. And unless something like the data integrity boards are set up, I just don't see anybody enforcing that. Certainly, OMB isn't going to enforce it. And I don't know who else would.

Senator COHEN. You don't put much stock then in the statement that there haven't been any demonstrated abuses under the Privacy Act that have materialized? And, therefore, the fears that were expressed by you and others previously have really been unfounded?

Mr. PLESSER. I don't put much stock in that. Maybe it's good that we've brought a lot of attention to the area, perhaps slowed them down. And so that's one of the reasons why there's not a lot of abuses.

Also, I think that there have been some concerns and some demonstrations of how the system can work badly. And there are some policy disagreements. I personally think it's an abuse to use IRS records in a match.

Of course, Congress specifically mandated that, so there's not much I can say about that. But I think this is an area that demands a lot of oversight.

Unfortunately, I think Mr. Wright indicated that there are groups watchdogging this, and that's sufficient. I don't think that's right. The American Bar Association—certainly it was not set up as a watchdog on Federal agencies.

And I don't think any of the other groups testifying today are "watch dogs" on an ongoing basis. So I think there is a need to have some kind of oversight mechanism, to have remedies to make sure that abuses don't happen in the future.

It's a policy issue of whether we want our Government to act in this way. I think we can make policy choices without demonstrating a series of horror stories.

The rest of the bill I think satisfies most of the interests of the ABA. One section, of course, which was in the bill which was not in the ABA, is ABA recommendations into the Data Integrity Board. I think that the Data Integrity Board is a very crucial element of your bill.

I also very much like the concept of the matching agreement because it creates a negotiation process, including the bureaucracies. I think that's very much related to the Data Integrity Board.

I assume the model of the Data Integrity Board, at least partially, is the Defense Privacy Board. That has been an example of where in the bureaucracy, if it is put in a place to negotiate any matching request for DOD has to go through that group, that group negotiates, they work out agreements, they get written commitments. And that is the way this program should be operated.

I think the Data Integrity Boards, using the DOD model, would probably be a very effective tool. It was suggested this morning that the IG sit on the Data Integrity Board. That's a very good idea. Let them wrestle with some of these hard policy decisions.

That finishes my statement. If you have additional questions, I'd like to answer them.

Senator COHEN. You've answered all of my questions, Mr. Plesser. You have pointed out the basic problem we have in making this kind of policy. Congress, from time to time, is under pressure to create exceptions to the Privacy Act. Drug interdiction, matching now of IRS records to trap those people who are suspected of dealing with drugs, so we create an exception.

It's very hard to resist the temptation to say to those guys, "go ahead." What was happening is the old salami approach. We keep cutting off one section at a time.

And I won't deal with the drug program right now. It's being debated by the House and Senate. Once again, we are about to be formulating some sort of policy without stepping back to see what is this doing to individual rights of the citizens.

The purpose of holding these hearings and the purpose of having a bill is to try and focus attention. It's not obviously a very hot subject matter for today's discussion when we have Justice Rehnquist on the floor, but to me it's one of the most serious problems we have faced:

How do you reconcile the fundamental freedoms of the American people in the age of the computer?

I think we're ignoring the problem that is being created. And we need to use the computer. But we can't allow it to undermine the basic freedoms that we have cherished. I don't think we have looked seriously enough at it to date because we are forced to act on an ad hoc basis.

We just keep chipping away and chipping away, and there is the notion somehow that if you have done nothing wrong, what are you afraid of?

And to paraphrase Yeats, when he says:

"That rough beast slouching toward the Potomac," it's an IBM computer.

Mr. PLESSER. Thank you very much. Let me just say that those of us in the so-called privacy community really acknowledge and appreciate your participation, and your staff's participation in this area. I think it's made a big difference and it's a beacon of light to us.

Thank you.

Senator COHEN. Our next witness is Jerry J. Berman, chief legislative counsel of the American Civil Liberties Union. He also serves as the director of the ACLU project on privacy and technology.

Mr. Berman, if you would follow the precedent that has been set and summarize your remarks.

TESTIMONY OF JERRY J. BERMAN, CHIEF LEGISLATIVE COUNSEL, AMERICAN CIVIL LIBERTIES UNION [1]

Mr. BERMAN. Senator Cohen, let me try and do that. I have a long statement which I will submit for the record, including a lengthy legal memorandum. I want to cover some of those issues this morning.

But first of all, like other witnesses today, I want to commend you, Mr. Chairman, for your leadership in this area, for bringing public attention to it, and for drafting this significant privacy initiative.

I also want to commend Senator Levin for joining you in cosponsoring this legislation.

We consider enactment of this legislation, S. 2756, to be a matter of the highest priority. Computer matching, despite all of our privacy reservations, is now institutionalized governmentwide. Rather than continuing to call for a ban on computer matching or continuing to argue that it is illegal under the Constitution or under current statutes, we must recognize the fact that computer matching is fully legal, however abusive of privacy rights it might be, and that we must seek to vindicate privacy rights through the enactment of legislation such as you propose.

While we do not think the legislation is as far reaching as we would like, and while it may not fully address the issue that you mentioned this morning and which is outlined in the OTA's privacy study—the eventual creation of a de facto national data base containing personal information on every American citizen—I think we have to move forward.

We want to achieve reforms. We are anxious to enact legislation to change the law, and to not have a model bill sit here in the Congress. In this regard, I am somewhat optimistic.

Over the last year there have been a number of privacy advocates and Government officials who have talked about computer matching under the auspices of our privacy project, the ABA and the Office of Technology Assessment, and while I think that there are differences of interpretation and the need for modification, your legislation embodies a series of fundamental principles and a framework which I think is almost assured a consensus between the government agencies and privacy experts, so that in fact, if we work very diligently on this legislation, we will achieve very significant and new legislation.

---

[1] See p. 104 for Mr. Berman's prepared statement.

I want to briefly point out that over the years we have come in and testified that computer matching violates the U.S. Constitution, constitutes a general search under the fourth amendment, violates the presumption of innocence, and violates the Privacy Act of 1974.

Nevertheless, computer matching has grown by leaps and bounds. It has tripled in the last 4 years. There are 110 ongoing programs under the OTA study. There isn't a week that goes by that there isn't a new notice of a computer match in the Federal Register.

It is important for civil libertarians and important for our organization to understand the legal vacuum that we are operating in. Computer matching is not considered a general search under the Constitution and courts have not recognized a privacy right in the records held by third parties. The fourth amendment has not yet been brought into the 20th century, and I doubt whether any court—including this Court with the new justices being confirmed—will ever recognize matching as a general search under the Constitution.

The best argument against computer matching is that it violates the Privacy Act of 1974. I think the drafters had in mind that when records are collected for one purpose and used for another purpose, citizens should be notified and that they should consent to that exchange of information. This is embodied in the Privacy Act, and I think the drafter, Senator Ervin, foresaw the coming of the advanced technological computer age when he said that this is the kind of abuse the drafters had in mind.

But as we all know, that is complete on the record. The Privacy Act has been overcome by the interpretation of the act's "routine use" exemption. As Mr. Plesser has pointed out, the remedy sections under the Privacy Act are unenforceable, and so computer matching continues in a legal vacuum.

The OTA study points out that oversight has dwindled to being nearly nonexistent, and thus administrative and internal checks do not exist.

So we turn now to say we need legislation. What we see your staff doing is essentially returning to the Privacy Act of 1974 and implementing the fair information practices and policies which the framers outlined and which they intended. We don't view it as radical legislation.

If you listen to the Government witnesses, many of the requirements for security procedures, matching agreements, and so forth are all embodied in current regulations. Although there are new requirements, which we will go into, which will create an added burden on the Government, the principles of notice, verification, and opportunity to be heard are fundamental due process principles, and we think that the Government has conceded that they are. The issue is how to get them embodied in law so that, across the board, there is a common understanding of what is meant. That is what this legislation will do.

Let's take the important provisions—matching agreements.

The importance of the matching agreements here is that they perform the function of making the Government think through their legal justification for matches. They also provide the possibility for both agency data boards and congressional oversight. I think they refer to the agency as watching the Federal Register notices, and we can tell them what is going on.

You cannot tell by reading a Federal Register notice today how intrusive a match will be when you find out this morning that in order to check on overpayments or underpayments under Medicaid they are looking at a number of data elements which may actually intrude on the doctor/patient relationship or at least raise the question. You cannot tell how intrusive the match will be by looking at the Federal Register notice, and neither the ACLU nor the ABA could even begin to start commenting.

What this legislation will do is lay out how many data elements are involved, what type of privacy protection will be provided, and the purpose and justification for the match. Then we can comment, you can comment, and the Data Protection Board may make modifications.

As the ABA did, we would recommend that these match agreements also cover private source matches. For instance, private source agencies with medical records ought to be covered by matching arrangements when they are dealing with the Federal Government.

Also, Federal agencies are dealing with credit cards and credit companies such as TRW. In testimony before this committee in 1982, it was reported that the IRS was attempting to buy information from marketing agencies to match against IRS records in order to detect tax evaders. In that instance, those arrangements should be covered by matching agreements.

In terms of justifying programs, we think that elements that should be added to the justification requirement are: How effective the program has been in the past; how many hits; how much fraud has been detected; if it is a recurrent match; and if it is a future match. We should have some knowledge of the anticipated payoff they expect from the match.

We are not saying that cost/benefit analysis is a major privacy protection. It was in the original Carter administration regulation but taken out. We are not asking to change that but to give some sense to it.

To answer Senator Levin's question, OTA went and spent 2 years trying to answer that question: Is the cost justified? How much does it cost to investigate 6,000 hits which boil down to 380 real fraud cases?

Those figures are not available, but it can be done through the matching arrangement.

The important provision in this legislation stressed by the American Bar Association and by the Government witnesses is actual notice to citizens of how information about them is being collected, exchanged, or verified.

Notice in the Federal Register is not notice at all. No one reads it. I hardly read it. I have it clipped for me, and I have a pile on my desk every year of new, unintelligible computer match notices.

When notice does appear on forms, it is often unintelligible. I read this one. A veteran applying for a benefit reads this:

> The information submitted may be disclosed outside the Veterans' Administration only as permitted by law, including the routine uses identified in VA System of Records 58 VA 212128, compensation, pension, education, and rehabilitation records VA published in the Federal Register.

That is not plain English. That is bureaucratic gobbledegook, and it obscures for citizens where their information is going.

In addition, some agencies, for example, under even the DEFRA regs disclose that collateral sources be contacted. Other agencies don't disclose that they will go to collateral sources to identify information.

When Congress sets forth a verification of applicants across the board, then you begin to get uniformity.

Notice, we believe, under the statute, should also advise citizens of the rights that the statute provides. They have a right to correct information. They have a right to refute information. They may have hearing rights at some point. Very seldom is the basic privacy right that you have the right to correct information that goes in your file explained to citizens in any form or in any way.

I think that very few citizens are aware of this privacy right. It ought to be made a part of the notice requirement now. We should say that you should have actual consent in addition to notice, even though we are not going to get that in this legislation.

But notice on the form, in clear, plain language, at least makes implied consent to acceptance of benefits meaningful in some sense, so that citizens can at least know that the cost of accepting a government benefit is that information will be shared with other agencies and maybe even the private sector.

Now, the Government has talked about the new burden of a notice provision, but as Mr. Plesser pointed out, and we agree, they should embrace actual notice. If citizens know that their records are going to be matched or checked against either their income records or other files, they are going to be more likely to put down correct information. It is going to deter fraud. The Government should not be displeased that notice would stop a doctor from double billing. That is the purpose of this program.

So notice serves both the due process function and it benefit the Government through fraud reduction. Thus, actual notice should be included in the legislation, and there should be no waiver of notice.

When we come to verification, we think that independent verification is important and ought to be spelled out in the statute. Independent verification deals with the issue that civil libertarians have often raised, that these computer matches violate the presumption of innocence because citizens' benefits are terminated on the basis of them. If there is independent verification, the presumption of innocence is preserved.

More importantly, by spelling it out in the statute we begin to get some uniformity. While the DEFRA regs say that verification is occuring, some agencies are verifying benefit programs against the unearned income data of IRS because it is required in the statute, but they are not going to verify other sources, such as wage and benefit data.

State officials will tell you there are potentially large error rates in those figures and all income data needs to be verified.

We point out that even the IRS data, which is supposed to reduce the error rate, has large problems in it.

GAO has just recently testified that because of the software problems with certain banks, they have inadequate unearned income data reported to the IRS which affects over 1 million taxpayers. If this data is used by the welfare programs, it affects those persons receiving benefits.

So verification is an important auditing tool, as well as an important due process right.

Now, one addition to the statute would be reasonable time for verification. The DEFRA regs do provide time.

Bureaucrats and State officials are arguing that the time limits need to be lengthened, but time limits should also require that at some point if they exceed their time limits the benefits should not be denied. The applicants should be paid pending final verification. If the Government can't verify its own information, the burden should not fall on the applicant.

I believe that provisions like this are in the final regulations of the INS program. Knowing their data base is so full of inaccurate information, they would say, "Do not rely on a hit. Verify first—pay first and verify later." I think that is established in the statute.

Other protections in this statute in terms of matching agreements go to privacy and security of data and destruction of data to ensure that it is not merged. We think these are important provisions. Some of them also are in the DEFRA regs.

In talking to Federal and State officials in the age of microcomputers with increasing online access to information and new networks of information, it seems information is increasingly vulnerable. There is very little being spent in terms of time or personnel for oversight.

So, privacy protections need to be put in, which brings us to the data integrity boards. We think that these boards—and we agree they are subject to restructuring to make sure that the Inspector General has all his prerogatives and also is part of the oversight process—are the central part of this legislation.

Many would say that the failure of the 1974 Privacy Act is due in large measure to the failure to create a broad oversight board. I don't think there is support for a broad oversight board, and I am not even sure it is a good idea. But the data integrity boards with their limited function of watching over matching verification programs, as spelled out in this legislation, are essential to ensure proper oversight.

You asked Mr. Plesser if the sanctions are adequate. The sanctions in this legislation, in addition to whatever the Privacy Act provides, provide that they stop exchanging records.

For 12 years, that's been the rule with respect to inaccurate arrest records at the National Crime Information Center. However, States have not stopped exchanging inaccurate or incomplete arrest records.

The law enforcement prerogatives and the benefits on integrity needs will always have adverse impacts on privacy. There will be mistakes that will be rectified and the records will be exchanged.

Two things can be done, however. One, as part of the function of the Data Integrity Boards, is to make them disclose to the Congress not only what kind of procedures they have included, but also if they've discovered any violations of their matching agreements which violate citizens' privacy and due process rights.

So, while they may have corrected it, Congress may also want to make modifications.

Two, I would consider changing the penalty structure in the Privacy Act to provide for statutory damages. There is no way to vindicate privacy rights without liquidated damages.

The Federal Wire-Tap Statute gives every citizen $1,000 for actual damage as a result of a wire tap. It's very difficult to put an actual damage figure on the results of a wire-tap, a search through papers or the breaking down of a door.

Here, a modest statutory damage award would at least give citizens some remedy to vindicate their rights.

Finally, I mentioned at the start that I think that this legislation is important. Essential. But it does not address the long-term development towards a de facto national data base.

I just want to make a couple of comments and conclude that. If the statute is enacted, it will only control computer matching. It won't halt it.

Under these programs, matching is going to expand. The trend is toward front-end verification systems. Front-end verification systems reduce payment errors and allow them to get on top of the situation early.

The Deficit Reduction Act started us on the road toward that. And I think it's the way of the future. Some argue that it's less intrusive on privacy because it's individualized, each applicant is looked at and there's no searching through a ream of files.

In fact, verification will always be done with matching. But my view is that front-end verifications raise far more fundamental civil liberties issues than computer matching. I do not believe that computer matching is a general search under the Constitution, or even as described in the current technology.

And I'll be prepared to explain that. But, front-end verification depends on quick and accurate benefit determinations. And these determinations may save taxpayers money and they may serve the citizens' interests in obtaining benefits as soon as possible.

But they require more complete and accurate information. In establishing the IEVS system, the Government required more program information, wage income, and IRS income data to be made available at the front end.

They may require standard formats to be developed. They did not require computerization, but if you read the regs and you read the regulation statements, you'll see there is a drive toward computerization.

And now there are programs working to overcome the technological barriers to on line access to this information. We agree with OTA that this is leading toward the development of a number of de facto national data base systems.

As you know, in the 1960's the Johnson administration proposed having one central data file in a main frame of all census, tax and income data to serve the welfare of the State. It was attacked as big brother government and roundly condemned and abandoned. Under the verification systems, on line access and networking information can be left in decentralized locations and assembled at a centralized location by having POM formats.

That's what happens with front-end verification. And, the system's going to grow. The administration is adding programs to the system under the Payment Integrity Act proposal.

Certainly, in the near future, the FBI will want access to the data base for its purposes. The INS will want to attack illegal aliens through it. There will be more and more pressure for 1040 information to be included as part of that data base.

There's going to be new efficiency in Government. But we believe that there are some fundamental civil liberties costs that will be paid. We don't know what they will be, and I don't think it's all-encompassed simply in terms of privacy. Something more fundamental is on the line.

And I think it's our sense of individual liberty itself. Information which could have been lost in a file drawer 10 years ago is now retrievable. Immutable records can impact on how we behave, whether we dissent, how we lead our lives.

Deviation calls attention to ourselves in the computer age. You don't want to make mistakes and you don't want to deviate because that's a hit in some future computer match, or verification program.

Our sense that we could begin again in America may be lost forever in the computer age.

And it's really time that we pay attention to this growing problem and recognize it. I want to quote Senator Ervin, who put it best in his hearings on data banks in the 1970's:

> These new sciences increase power to discover and report immediately the activities, thoughts and philosophy of an individual at any given moment in time. That picture of a person is recorded forever, no matter how a person may change as time goes on. Every person's past thus becomes an inescapable part of his present and future unless new controls are enacted, new legislative remedies are provided, and unless Federal officials can be persuaded to exercise more political self-control, this country will not reap the blessings of man's creative spirit, which is reflected in computer technology.

This legislation will help us focus on the problem. If we could make two changes by eliminating the routine use and requiring as part of this legislation that outside of routine records now being used for match, any future record must be authorized by Congress, so that Congress can weigh the privacy impact of adding either to matching or verification systems, that would be a step in the right direction.

Along with the ABA, we would recommend reestablishing in this legislation that tax information, census information, sensitive information, sensitive political information should not be used for matching and verification programs.

These are steps. If this legislation is enacted in a few years, when the oversight mechanisms are in place, there will be more privacy and more due process protections. But I think we will be in a better position to take a new look at these long-term consequences.

We support the legislation. We're anxious to work with you and the Government to achieve consensus. We again thank you for this opportunity to testify today.

Thank you, Senator.

Senator COHEN. Thank you very much for summarizing your lengthy written statement. I want to commend you and the ACLU for the scope of the testimony you've given me. I don't know of any other organization that's taken more unpopular positions over the years, but have done so to remind us of the importance of the rights that you are trying to articulate.

Our final witness today is Priscilla Regan, who represents the Office of Technology Assessment. Ms. Regan is the principal author of the OTA's report, entitled "Electronic Record Systems and Individual Privacy," addressing many of the issues we are studying today.

TESTIMONY OF PRISCILLA M. REGAN, PH.D., OFFICE OF TECHNOLOGY ASSESSMENT[1]

Ms. REGAN. Mr. Chairman, thank you for the opportunity to appear before your subcommittee this morning to discuss the findings of OTA's report on Electronic Record Systems and Individual Privacy in the context of the Computer Matching and Privacy Protection Act of 1986.

The OTA report is part of a larger study of the effects of Federal agency uses of information technology, particularly their effects on civil liberties and congressional oversight.

As part of this study, OTA conducted a survey of 13 cabinet departments and 20 selected agencies. Among OTA's findings were the following:

First, only about 13 percent of Privacy Act record systems are audited for quality, especially the accuracy of the data.

Second, the Federal inventory of microcomputers increased from a few thousand in 1980 to over 100,000 in 1985, and only a few percent of the agencies reported revising their Privacy Act guidelines with respect to microcomputers.

Third, 33 agencies reported less than one person per agency assigned to the Privacy Act implementation. And 34 agencies reported only one person.

Fourth, 11 Cabinet level departments and four independent agencies reported conducting 110 matching programs, with a total of approximately 700 separate matches from 1980 to April 1985.

In the 5 years from 1980–1984, the number of computer matches nearly tripled.

Fifth, in 20 percent of the matches, agencies provided information on the number of records matched, for a total of over 2 billion separate records.

In analyzing the survey results, and after discussions with officials from a number of Federal agencies, OTA reached three general conclusions:

---

[1] See p. 125 for Ms. Regan's prepared statement.

First, new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves.

In the 12 years since the act was passed, at least two generations of information technology have become available to Federal agencies.

These technological advances have opened up new opportunities for improving the efficiency of Government recordkeeping, the detection and prevention of fraud, waste and abuse, and law enforcement investigations.

At the same time, the opportunities for inappropriate, unauthorized or illegal access to and use of personal information have expanded.

Computer matching is a good example of the conflicts between the Privacy Act protections and new uses of information technology. Computer matching would appear to be discouraged by the act's requirement that information collected for one purpose not be used for another purpose without the consent of the individual.

Yet, computer matching has been defined as a routine use and is exempt from this requirement.

The Privacy Act also requires agencies to collect information to the greatest extent practicable directly from the individual; yet, in computer matching, information is collected from third parties.

This increases the possibility that inaccurate or incomplete information will be used.

Second, OTA found that there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with the Privacy Act and related OMB guidelines.

There are few internal agency checks on computer matching and front-end verification. Program personnel appear to have substantial discretion in deciding whether or not to use these applications.

With respect to external oversight, OMB has developed a number of procedural guidelines for computer matching. But OTA concluded that there is no oversight of agency compliance with these guidelines. In effect, the guidelines could be ignored.

OMB has adopted a very passive role. In addition, Privacy Act officers in most agencies do not have the stature or the time to monitor compliance with OMB guidelines. At present, there are no general Federal guidelines, statutory or administrative, for the use of front-end verification.

Third, OTA found that neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency and law enforcement implications of Federal electronic record systems can be fully debated and resolved.

Since the Privacy Act was passed in 1974, the primary policy attention has shifted away from privacy-related concerns. Interests in management efficiency and budget have dominated the executive and legislative agenda in the late 1970's and early 1980's. Congress has authorized information exchanges among agencies in a number of laws.

In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

Given the emphasis being placed on Federal management and efficiency, and the sparse oversight of the Privacy Act, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

OTA identified a range of policy options for congressional consideration, including those that deal with specific problem areas, and others that address institutional changes.

If Congress were to do nothing at this time, then the present policy problems and confusion will continue. In addressing specific problem areas, for example, Congress could establish control over Federal agency use of computer matching, front-end verification, and computer profiling.

This is the approach that S. 2756 adopts. Other specific areas in need of congressional consideration include data quality, protections for sensitive categories of information, including medical information, use of the Social Security number as a de facto national identifier, and access to IRS information.

OTA found that strengthening an existing institution or establishing a new one would bring more visability to the issue of personal information collection and use.

This could achieve three purposes. First, an institution could play the role of an ombudsman in assisting individuals to resolve individual or class grievances with a Federal agency.

Second, it could oversee Federal agency compliance with the Privacy Act and related OMB guidelines.

Third, an institution could provide a forum in which the proposals to alter personal information practices and systems could be discussed.

OTA identified four institutional changes available to Congress. The first is to strengthen the role of OMB in the enforcement and oversight of the Privacy Act.

The second is to increase the size, stature, and authority of privacy staff in agencies.

Third, Congress could improve its own organization and procedures for consideration of information privacy issues.

And, fourth, Congress could establish an entity such as a privacy or data protection board to oversee the personal information practices of Federal agencies.

S. 2756 addresses many of the problems OTA identified with regard to computer matching and frond-end verification. The provisions of S. 2756 will make statutory the existing OMB requirement that matches be reported in the Federal Register. It also restores the requirements for a 30-day public comment period and for advance notice to Congress and OMB. S. 2756 also extends these requirements to front-end verification programs. Additionally, S. 2756 requires agencies to specify in the written agreements the procedures they will use to provide notice to individuals whose records are being used in a matching or front-end verification program.

The implication is that this notice would be in addition to the notice in the Federal Register; however, it is possible that an agency would specify its notice procedure as being the Federal Register notice. The OTA findings indicate that some notice more directly addressed to the individual is necessary to conform to the goals of the Privacy Act. S. 2756 will require more direct notice to individuals before an adverse action is taken, because the information would have to be independently verified, either by the individual or a third party and because the individual would be given an opportunity to refute the information. The requirement for independent verification also addresses the existing problems of data quality and is an important step in minimizing the use of inaccurate or incomplete personal information.

With respect to institutional arrangements for oversight, the written agreements between the matching agency and source agency that S. 2756 proposes, would help to rectify the difficulties with lack of internal agency control.

The provision for an agency data integrity board may be the most important section of the bill, as it provides for an institutional enforcement mechanism.

It will be important that the data integrity boards not only approve the written agreements but also follow up to ensure that the terms of the written agreements are met. If the written agreements merely replace the present OMB check list, then they will not provide any additional means of agency oversight. It may also be possible to assign the data integrity boards a role in assisting individuals in finding out about the uses of personal information or in bringing questions, complaints or grievances to an agency.

The data integrity boards could provide a forum within each agency in which the tensions between privacy and efficiency could be debated and resolved. The membership of these boards will determine how effective they are in this regard. If the boards are to be balanced, they will need advocates of equal status and expertise representing both interests. Although the data integrity board is an important institutional change at the agency level, it does not provide a direct means for arriving at the comprehensive picture of Federal activities in this area.

OTA found that an overall picture is important to realizing the scale and scope of Federal personal information exchanges and uses.

In conclusion, S. 2756 addresses many of the problems identified in the OTA report. It is a significant first step toward exercising statutory control over Federal agency use of computer matching and front-end verification.

I would be happy to answer any questions you may have.

Thank you.

Senator COHEN. Thank you very much, Ms. Regan, for your testimony.

You indicated there is no entity that can address the emerging issues and trends to evaluate privacy cases.

What about OTA?

Ms. REGAN. We do studies at the request of congressional committees. We don't have an ongoing function in this area.

Senator COHEN. You don't think that the congressional committees are capable of carrying the work out?

Ms. REGAN. Excuse me?

Senator COHEN. The kind of oversight and monitoring that would be really necessary to be sure that these kind of issues are addressed?

Ms. REGAN. I think it would be very time-consuming for congressional committees to carry out that function. It is also difficult because many of these programs cross over many jurisdictional lines. And therefore, it might confuse the situation.

Senator COHEN. Earlier this morning, Mr. Wright indicated that one of the criticisms of OMB's oversight computer matches is that in no place did OMB ever stop a match.

Ms. REGAN. That is true.

Senator COHEN. Is that an adequate basis for OMB's oversight functions right now? I don't understand what the point is that in no case did OMB ever stop a match. Does that mean that matches are all meeting existing standards?

Ms. REGAN. I don't think that would be an indication that all the matches meet OMB standards.

The OMB guidelines give OMB the authority to issue additional guidelines or even regulations. OMB hasn't really taken a more aggressive stance in issuing regulations or in reviewing matches that have been proposed in the Federal Register and denying an application for a match. The process right now is really just one of OMB serving as a clearinghouse, but not as an overseer.

Senator COHEN. Ms. Regan, I don't have any more questions, but I have just a couple of comments to Mr. Berman, who is still sitting here.

As usual, Mr. Berman, I commend you and Ms. Regan for sustaining yourselves throughout the whole testimony.

One of the ironies here is, here we have one of the most conservative administrations in recent years—but maybe it is not fair to characterize this administration or any administration, I suppose. It started in the Carter administration, because of the pressures on finances and budgeting pressures and the pressure of technology, but we appear to be drifting to the right, so far to the right that we're actually going to be joining hands with the left. That is one of the great ironies. And I find there are many things going on in our society. When the ACLU raised the issue of privacy, what they are saying is that when you diminish the significance and the importance of privacy, what you are doing is subordinating the individual to the State. You are well on the way to a socialized state of being.

I indicate that in terms of DRG's. By way of example, we've got a problem with DRG's. We can't afford any more of them. So we set up these designated groups. If you fall in that category, then you serve a formula.

What we are doing is, we are socializing medicine to that degree, that we are starting to treat people, not as individuals, but as fungibles, if they fall within certain categories, that is all you get for that kind of injury, that kind of treatment. And it really alerted me today, when I heard the statement being made that we are using computer matching to now perhaps monitor the quality of care being extended to individuals.

What are we doing getting into private medicine? Look at it in the insurance business, because we've got an insurance crisis now. We are now talking about stepping in and modifying the historical notions of tort law.

What we are doing is, we are talking about eliminating any consideration for pain and suffering or putting a standard amount of money for pain and suffering, and what we are doing is socializing injury. We are treating every single individual the same without recognizing extensions. A person who might be a gifted pianist, who loses a finger, ought to be treated somewhat differently than perhaps a carpenter or a mechanic or a surgeon, but we are starting to lose distinctions between individual rights, because we are now treating them all alike, and that is a great danger.

And the same thing, I think, is true when we are talking about shifting the burden of proof in our Government and in our society. We are no longer presumed to be innocent. Now the pressure is on to start polygraphing everybody who has access to any kind of information that might be deemed sensitive. I don't know how many million people—about 4.3 million people perhaps—who are lining up and taking a urine test periodically. The burden of proof is shifting to us to show to the State that we are innocent.

And this is part of that. This is not separate and distinct. It is part of a concatenation of events that is building and leading us to the conclusion that the State should be able to determine the lifestyle and monitor the activities and determine what is acceptable or not acceptable, all in the name of efficiency.

This bill is not adequate in itself. We are not going to stop that. And I commend Mr. Berman for his yielding to practicality, I guess, because the ACLU has not been accused of that in the past of always being practical, but they've been persistent in what they've advocated. It has forced us to stop and look as to what is happening to the freedoms we cherish. And again, what is so ironic about it is here we have an administration and a President whom I believe articulates the basic ideas of this country in talking about human freedom, individual freedom, rolling against the kind of Communist state that exists behind the Iron Curtain or might exist down in Nicaragua.

And yet through our own policies, we are drifting very close to adopting the state being all powerful and the individual rights being subordinate to the interests of the state.

This bill or any modification I have made to it or perhaps even any to the Privacy Act is not going to change that, but I think somebody, many of us ought to be raising our voices in objection. We can't stop the rushing technology. We can't stop it any more than we can stuff time back in the bottle, any more than we can stuff technology back in the bottle, but we have to be concerned about more: How cost efficient it is and how cost effective it is. We have to be concerned about where are we going as a society, when we have to prove our cases or establish our cases, when we have to prove that we fall into a DRG or to have individual rights to bring suit against a doctor who leaves a scalpel inside your intestine during the course of an operation, but there is no pain and suffering allowed.

That is the kind of thing that is taking place across the boards. It's not just computer matching. It is much more widespread.

But I want to thank you and Mr. Berman and all the other witnesses, and Joe Wright and the others who were here. Hopefully, we can fashion a bill that will be acceptable.

Thank you very much.

[Whereupon, at 11:55 a.m., the hearing was adjourned.]

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Tuesday, September 16, 1986

STATEMENT
of
JOSEPH R. WRIGHT, JR.
DEPUTY DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET
Before the
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT
of the
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here this morning to discuss S.2756, a bill that seeks to put into statute procedural steps for the use of an important tool in our campaign against waste, fraud and abuse - computer matching. With me is Richard P. Kusserow, the Inspector General of the Department of Health and Human Services and the Vice Chairman of the President's Council on Integrity and Efficiency.

While we have serious concerns about the bill and think that substantial changes are needed to make it workable, it does contain elements of a balanced approach to solving many of the problems related to the use of this technology. On the one hand, it clearly authorizes the government's use of computer matching by amending the Privacy Act of 1974 to permit disclosures of information for matching purposes. On the other hand, it requires that matching programs include a number of procedural due process steps to preserve the rights of the subjects of any matches.

We certainly support the basic thrust of the bill, especially since it seems to incorporate an approach that we developed years ago and continue to apply in a variety of programs. I want to state at the outset, however, that we do not yet fully understand how the bill's procedures will work in practice, nor exactly what effect they will have on the way our programs are operated; although, later on in this statement, I will point out some areas that we think will be troublesome. As we study the provisions and gather information from the agency program officials and the Inspectors General, we will have a much clearer idea about the kinds of changes that are needed to make the bill work.

Having workable procedures is very important to us because our experience suggests that the imposition of excessive and let me stress the word excessive, administrative procedures will discourage matching. We have found that computer matching is an extremely productive tool in our efforts to prevent, correct and recover erroneous payments in agency programs. Let me give you some idea of the size of the problem we face. While most programs do not measure payment errors, those that do find that between 4 and 20 percent of all payments go to ineligible persons or constitute overpayments to eligible beneficiaries. In 1984, the Federal share of erroneous payments was about $900 million in the Food Stamp program, $500 million in the Medicaid program, and $485 million in the Aid to Families with Dependent Children program, to take three examples. That is a total of nearly $2 billion disbursed in error, out of expenditures of about $42 billion. These erroneous payments are made because of beneficiary errors in reporting income and assets in means-tested programs, use of fraudulent identification documents, and duplicate payments. These errors are of a kind that computer matching is particularly suited to detect and prevent, e.g., in AFDC programs, matching (in conjunction with other management improvements) brought error rates down from 11.1% in 1975 to 6% in 1984. There is simply no way that we could achieve this kind of reduction without resorting to matching. I will give some specific examples later in my testimony.

Moreover, the Congress has demonstrated its understanding of the problem and support for matching by enacting the Debt Collection Act of 1982 as well as the Deficit Reduction Act of 1984. Provisions in both of these acts work to encourage agencies to reduce error rates and their excessive costs through the use of automated matching. It is important that we not now create unneeded barriers to its use. If we do, the errors will again rise and program costs will increase as we provide services to those who do not deserve them.

BACKGROUND OF MATCHING

EARLY HISTORY AND DEVELOPMENT OF OMB GUIDELINES

To dispel any concern that matching, as done by the Federal agencies, is taking place in an unregulated environment with inadequate oversight, it is critical to understand how our present procedures came about, the value of matching, and what we are currently doing to guard against misuse of matching.

By 1981, this valuable tool in the fight against fraud, waste and abuse had fallen into unfortunate disuse. To a certain extent, it was a victim of bureaucratic overcautiousness brought about by uncertainty - uncertainty about the effectiveness of matching, about whether the Privacy Act of 1974 permitted the data exchanges necessary to conduct matching programs, and about where the Congress stood on the issue.

But, when computer matching came to the attention of the public in the late 1970s automated auditing was hardly a new process. Agencies had for years been conducting internal financial audits of their programs for quality control purposes. What was new about programs like (then) HEW's Project Match was that their focus on fraud, waste and abuse detection and prevention required the sharing of data across agency boundaries, an activity that triggered privacy concerns.

We need to remember that the Privacy Act, a statute we are now familiar with, had only been in operation for a few years at that time. Agencies were working to incorporate its principles into their daily operations without a great deal of certain knowledge about its effects on their programs. Little case law had emerged to provide needed interpretations. The only written guidance came from OMB in the form of Implementing Guidelines.

Many agencies at this time were not comfortable with the idea of such data sharing, especially in an automated environment. They remembered that one of the primary forces that brought about the Privacy Act was a concern about the potential effects of automation upon the individual. Indeed, the set of concepts that provided the intellectual foundation of the Privacy Act, the so-called Code of Fair Information Practices, evolved from the work of a 1972 advisory committee on automated personal data systems commissioned by the Department of Health, Education and Welfare. There was a genuine concern, expressed in the preamble to the Privacy Act itself, that the computer had the capability "to greatly magnify" the harm done to the individual. Thus, restrictions on the uncontrolled sharing of personal data among agencies were added to the Act. These restrictions acted as a brake on the development of matching programs, since agencies were not certain that the Privacy Act would support the data sharing necessary to conduct such programs.

The Privacy Act established as a basic premise the principle that an agency should obtain written consent from a record subject before disclosing his or her records. Recognizing that a totally unthinking adherence to this principle could prevent the government from disclosing when information was necessary to protect the public interest, the Congress wisely wrote into the law a series of narrow exceptions to the written consent requirements. One exception permitted disclosures without consent if they were for a "routine use," and it was under this exception that most data transfers for matching purposes took place. This exception in the Privacy Act defined a "routine use" as a use that was compatible with the purpose for which the agency originally collected the data. The vagueness of the term was offset by a requirement that agencies publish their proposed routine uses in the Federal Register where they would be subject to public scrutiny and comment.

While compatibility was the standard that controlled disclosure, it was not defined in the Act; nor, as I noted earlier, was case law at this time at all developed on the issue. Thus, early in the agencies' implementation of the Privacy Act, concerns over whether compatibility could truly be demonstrated caused some agencies to decline to participate in several matching programs.

It was clear that standards for matching programs were needed, and in 1979, in an effort to bring procedural consistency to the agencies' use of matching, and to enforce a discipline on the process, OMB issued "Guidelines on the Conduct of Computer Matching Programs." The effect of these Guidelines was to legitimatize matching if it took place within the provisions of the Privacy Act but to disallow it otherwise. The Guidelines provided rules that the agencies found useful in implementing matching programs. Moreover, Congress itself looked on the 1979 Guidelines as providing a needed procedural structure in which matching could take place. The legislative history of the Inspector General Act of 1978 shows that the drafters expected that OMB's proposed "Matching Guidelines" would be followed by the new Inspectors General in conducting any matching programs in order to ensure a "useful balancing of the competing values [protection of privacy vs. governmental efficiency]....Matching programs will occur, but only in conformity with the protections contemplated by the Privacy Act."

The Matching Guidelines were designed with two basic goals in mind:

- To require that the agencies themselves, the public, the central management agencies and the Congress understand and evaluate matching programs before they took place; and

- To create a uniform set of procedures for agencies to follow in conducting matching programs that would ensure that agencies conformed to Privacy Act requirements for data sharing.

The oversight procedures consisted essentially of publication and reporting provisions. Agencies were required to publish notices describing proposed matching programs as well as any routine uses associated with these programs to solicit public comment. They were also required to report matching programs to OMB and the Congress 60 days in advance of their implementation.

The uniform procedures covered both interagency matches as well as intra-agency matches to combat fraud, waste and abuse. However, matches for administrative or statistical purposes were not covered. The procedural steps took agencies through the process of determining whether to do a match; and if so, how to do it. The preliminary step required the agency to complete a benefit/cost analysis that included an analysis of alternatives to matching and an explanation of why the alternatives were not chosen. In the remaining steps, the agency was required to define the data to be used, prepare the Federal Register notices for new systems or routine uses, and finally terminate the match and dispose of the materials used. "Source" agencies were cautioned to review material they were asked to provide to the agency performing the match to determine the appropriateness of the matching program. Sources were also cautioned to have in place the appropriate Privacy Act systems of records and routine uses before participating in any matching program.

During the 3 years that these Guidelines were in effect, OMB received 20 matching reports. The Departments of Agriculture and Health and Human Services submitted 75% of the reports, most of which reported programs designed to uncover fraud and abuse in Food Stamp and Aid to Families with Dependent Children programs. Indeed, a follow-on to HHS's "Project Match" which was the progenitor of modern matching programs was among these. The Department of Education and the Veterans Adminstration accounted for the remaining 25%.

Because the Guidelines were new and their procedures untested, OMB staff spent a great deal of time in contact with agency personnel working out the details of what was needed to comply with both the Matching Guidelines and the Privacy Act. The ultimate agency report to OMB and the Congress was simply the documentation of that close coordination. In no case did OMB review of these reports reveal any violation of either the Privacy Act or the Matching Guidelines because great care was taken before hand to make sure a violation did not exist.

Moreover, these Guidelines appeared to have satisfied both Congressional and public concerns over matching. Few public comments were ever generated by agency publication of proposed matches; comments that were received raised no substantive concerns.

The Guidelines, while allaying to a certain extent, agencies' concerns about the legality of matching, had their own problems. They were unnecessarily expensive and administratively difficult for agencies to implement. They were hard to understand. Moreover, despite reassurances, some agencies remained concerned about the propriety of this kind of data sharing and were reluctant to participate in broad-based interagency matching programs. Thus, after a promising beginning, computer matching of the Project Match variety gradually faded away and languished until the early 1980's.

EFFORTS OF THE PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY TO REVITALIZE MATCHING

This Administration recognized the value of this tool very early. In March of 1981, President Reagan established the President's Council on Integrity and Efficiency (PCIE), an organization that took the lead in revitalizing matching to fight waste, fraud and abuse. Composed of the statutory Inspectors General and representatives of other major Federal executive agencies, the new Council immediately began to consider major initiatives to fulfill the President's Executive Order. It is a group which I chair.

As a result, in the past 6 years, matching has evolved from a somewhat controversial and misunderstood process into a mature and rather routine albeit very successful one.

One of the first major projects the PCIE undertook was the Long Term Computer Matching project, co-chaired by the Inspectors General of the Department of Health and Human Services and the Department of Labor. Dick Kusserow, the Vice-Chairman of the PCIE, personally took the lead in that project. The major goal of this project was to promote the cost-effective use of computer matching to combat fraud, abuse and erroneous payments in federally funded programs. Through its membership of Federal and State program administrators, the project sought to:

- gather and share information about Federal and State matching activities;
- identify and remove technical and administrative obstacles to computer matching, while preserving essential protections and safeguards to personal data; and
- foster increased Federal and State cooperation in computer matching activities.

One of the project's first tasks was to recommend ways to improve the OMB "Guidelines for Conducting Computer Matching Programs;" to streamline the paperwork requirements while preserving the requirements for privacy and security of records. The revised guidelines, issued on May 11, 1982, incorporated many agency recommendations for clarification and change based on their actual operating experiences. While streamlining the paperwork requirements for justification and approval, the revised guidelines preserve the requirements for Federal Register notices and strict safeguards concerning use, storage, and disclosure of information from matches.

As further guidance to agencies in complying with the Privacy Act and the 1982 Guidelines, the PCIE developed a "Model Control Systems and Resource Document for Conducting Matching Projects Involving Individual Privacy Data." This document provides an approach to conducting computer matching that meets the requirements of the OMB Matching Guidelines. Specifically, it provides a methodology for assuring adequate protection of personal data during computer matching and presents a model set of processes and procedures for use when undertaking computer matches.

On December 29, 1983, OMB issued to all Federal executive agencies this document and the "Computer Match Checklist" which is to be completed by each agency engaging in or providing data for computer matching of Federal, State or local entities. The checklist was designed to ensure documentation of compliance with Privacy Act and OMB Matching Guidelines. The checklist must be completed and maintained for use in annual submissions to OMB under reporting requirements of the Privacy Act, as well as for review by OMB, GAO or others to ensure safeguarding and prudent management decisions regarding matching.

The PCIE Long Term Computer Matching Project has also done much to advance the cost-effective use of computer matching techniques in detecting errors and verifying eligibility for government programs. For example, the project included a catalogue of both State and Federal use of computer matching and related techniques, including State use of front-end verification techniques. These inventories served to document the extent of matching at the time and to heighten awareness to the array of possible applications of the technique.

There are additional examples of what the Long Term Computer Matching Project has done to promote efficient and secure matches.

o The Computer Matching Newsletter is a quarterly publication designed to promote the sharing of computer matching technology and applications among Federal and State agencies.

- The Standardized Formats, developed to facilitate State computer matches, created standardized data elements and record formats. These are now being used in the implementation of the 1984 Deficit Reduction Act requirements, which I will discuss later.

- The Manager's Guide to Computer Matching, which contains a methodology for cost and benefit analysis, provides managers of State benefit programs with a practical guide to conducting matches.

- Project Clean Data is a computer program that can be used by Federal, State and local agencies to increase the integrity of personal files by identifying incorrect or bogus Social Security numbers.

Beyond the issue of safeguarding personal data in the conduct of computer matches, the PCIE is also sensitive to the security of computer systems. So, in 1981, the Computer Security Project was initiated and has operated in tandem with the Long Term Computer Matching Project. The major goals of the Computer Security Project were to document known cases of computer-related fraud and abuse, identify common vulnerabilities, and develop methods to assure the integrity of Federal information systems and State systems administering Federal programs.

One of its first initiatives was a two part study of computer-related fraud and abuse. Initially all Inspectors General were surveyed to identify all known cases of fraud and abuse that involved government computers. Beyond identifying 69 fraud and 193 abuse cases, the survey was able to document a number of generic vulnerabilities in government computer systems. The second phase of the study involved the interviewing of 46 perpetrators of computer related fraud. Those interviews provided new insights in the who, how, and why of these crimes.

The PCIE has also studied the integrity of electronic media billing, and conducted a security seminar for Inspectors General and Assistant Secretaries for Management. In the coming fiscal year it will initiate studies to assess computer security in State agencies administering Federal benefit programs, improve the auditability of computer systems, and survey system life-cycle integrity and control requirements.

CURRENT SUCCESSFUL MATCHING PROGRAMS

Since 1981, the way in which the PCIE and the agencies use computer matching has matured. Agencies appear to be careful to assess the cost-effective potential of matches and to follow the procedural requirements. It is important to emphasize that we have had no evidence of any Federal abuses in computer matches and in the many Federal and State applications of matching, many substantial savings are evident. For example:

- The State of New York routinely matches welfare recipient records with quarterly wage reports and has estimated over a 300 percent return on the costs of this system.
- The Social Security Administration routinely matches its Supplemental Security Income files against the Veterans Administration's compensation and pension files, saving millions in erroneous payments and costly manual verifications.
- In 1982, the Department of Education ran lists of delinquent student loan debtors against Federal employee active and retired rolls and recovered $3.4 million.
- In 1985, Social Security files were matched with OPM pension files which identified individuals receiving payments from both systems without the proper offsets will result in $41 million in cost avoidances.
- In October 1985, the State of Missouri matched SSI data with Medicaid files to identify individuals who were residing in Medicaid reimbursed facilities but receiving full SSI payments. The match identified over $44,000 in overpayments

while costing only $10,000 to run.

- In July 1985 the records of four million SSI recipients were matched with IRS unearned income files (Form 1099). This match identified $117.5 million in overpayments for which recovery action was instituted. The full cost of conducting the match, including the cost of follow-up, is $6.4 million.

Certainly this array, and the many other examples, of successful matching projects helps to demonstrate the value of matching. The Congress apparently agrees and has demonstrated its support for the use of this technology in such legislation as:

- The Debt Collection Act of 1982 authorized several important applications for computer matching. Applicants for loan assistance were required to provide their taxpayer identification numbers (Social Security Account Number (SSN) for individuals) which enabled agencies to screen loan applicants or recipients against IRS delinquent tax files. Federal employee SSNs can be matched against the delinquent debt files of other Federal credit agencies. In addition, the Debt Collection Act authorized the IRS to release to Federal agencies the addresses of delinquent debtors to be used in collection efforts.

- The Tax Equity and Fiscal Reliability Act of 1982, in which

Congress set statutory targets for States to meet in reducing errors in public assistance programs -- 3% for AFDC and Medicaid by 1984. The Food Stamps Amendments of 1982 set a target of 5% for Food Stamps for 1985. All three programs were given interim targets beginning in 1980. Congress reacted to a lack of progress in meeting these targets by passing the income and eligibility verification provisions of the Deficit Reduction Act of 1984 (DEFRA).

o The Income and Eligibility Verification provisions of the 1984 Deficit Reduction Act. In proposing this legislation, the Congressional intent was to reduce erroneous payments in federally funded benefit programs. This legislation authorized the Social Security Administration's Supplemental Security Income (SSI) program and State agencies administering the Aid to Families with Dependent Children (AFDC), Food Stamps, and Medicaid programs to request and use data from IRS on unearned income (interest, dividends, etc.) in determining individuals' eligibility for assistance. DEFRA also reaffirmed and strengthened existing authority for AFDC and Food Stamps to use wage data from the Social Security Administration and from State Employment Security Agencies. It is important to note that underlying these data exchanges, the DEFRA provided specific protections against misuse, such as safeguarding requirements, notice of use of data, and independent verification of the IRS unearned income data. In a typical match, each month the States send their computer tapes, with records on individuals who have applied for AFDC, Medicaid, and Food Stamps in the prior month, to IRS to be matched against the IRS unearned income file. In the aggregate, this would result in about 250,000 records on public assistance applicants being matched against a file containing records on nearly 180 million individuals' unearned income like interest and dividends payments reported to IRS by financial institutions. Similar matching takes place at SSA. Although this process is too new to allow us to report quantified results, the Congressional Budget Office, prior to DEFRA passage, estimated that DEFRA matching programs would save $275 million in 1987.

We anticipate that as the Congress sees that matching programs like these are cost effective and are being conducted with due regard to the rights of those involved, it will consider other benefit programs for inclusion.

For our part, we will be proposing that a number of programs be allowed access to wage and unearned income data, Social Security and unemployment compensation data. These programs include veterans benefits and medical care, means-tested housing programs, child nutrition programs, maternal and child health block grants, student aid programs, health education assistance and health professions and nursing student loans, railroad disability retirement. Such an expansion of current coverage would, of course, include privacy and due process protections at least as comprehensive as those in DEFRA.

I think my testimony thus far has demonstrated why we think matching is such an important and useful tool and what we are doing to ensure that it is conducted in a way which comports with existing statutory protections such as the Privacy Act. I would like to turn now to a discussion of some of the specific provisions of S. 2756 and point out some of the troubling procedural problems our initial analysis has revealed.

ANALYSIS OF S. 2756 PROVISIONS AND COMMENTS

As I said earlier, we see S. 2756 as having two main goals:

- It seeks to establish uniform procedures under which agencies would perform matches so that the subjects of the matches are afforded due process;

- It seeks to establish a number of oversight mechanisms to ensure that agencies implement the bill's procedures.

Many of the provisions of the bill are drawn from existing OMB issuances, e.g., Guidelines on the Conduct of Matching Programs and Appendix I to OMB Circular No. A-130. While we would prefer to see them remain exclusively in regulation so that they can be more readily altered to fit changing circumstances, we think they are fundamentally sound and have no objection to their inclusion in this bill.

There are some new provisions, however, that we think may have negative consequences that the Congress did not intend:

- Section 2(b)(3) of the bill requires that matching agreements contain an assurance that "individuals whose records are matched will be notified of such matching program or front-end eligibility verification program and the procedures for providing such notice...."

  While we agree that individuals should be made aware of the uses of data they provide or data that is about them, we are concerned about the breath of this requirement. Read literally, it would mean that each time an agency wished to conduct a matching program, it would have to write to each individual whose records were involved. It would have to do so on a continuing basis, for example, for eligibility-for-benefits verifications even when the applicant had been advised that such checks would occur annually for as long as he received benefits. Such a procedure would turn matching from a relatively simple verification process to an ineffective and prohibitively expensive one. Few agencies would be able to use it. Let me give you some examples to illustrate the scope of this problem:

-- Currently, neither the Internal Revenue Service nor State tax agencies issue notices to individuals affected by matches conducted for tax compliance purposes under the Federal/State Exchange Program. If the Service were required to issue such notices, almost every taxpayer in the country would have to receive one or more. The postage alone would likely approach $20 million.

-- The SSI/VA match I cited earlier is designed to determine if any SSI beneficiaries are receiving benefits from the Veterans Administration that would affect the level of SSI benefits. This match is run six times each year and involves nearly 10 million individuals' records. VA estimates that postage alone for these six matches would total $10 million. Note that this figure does not include preparation and processing time for the notices. That is a significant amount of money to charge off to operating costs.

-- State Child Support Enforcement agencies routinely match files of absent parents with Federal, State and local files in order to locate parents who are not meeting their obligations to support their dependent children, many of whom are on welfare. In locator matches like these, it would be literally impossible to comply with a specific notice requirement, since the point of the match is to develop address information.

-- In matches done to uncover evidence of fraudulent behavior, such as HHS matches designed to uncover physicians who are double-billing Medicare and Medicaid for the same service, providing notice would alert those being investigated and permit them to alter their behavior long enough to avoid detection.

Moreover, what good does it do an individual to know that an agency intends to match data about him after he has provided the data? Such notice occurs at the wrong point in the process. The proper point is when he is about to provide the data and has the ability to decide not to, and Section (e)(3) of the Privacy Act already requires that individuals receive notice at this point. Admittedly, such notice is often fairly general, e.g., "we intend to check other data sources to verify the information in your application," but it does occur at the right time. It also serves a deterrent purpose by making an applicant think twice about supplying false data.

As to specific matching programs, our current practice is to publish a notice in the Federal Register. I understand that the Federal Register is not the most widely read journal; but it is essentially the "house organ" of the government and the place where we can put a more complete description of a matching program than can occur on an application form.

Once the match has occurred and reveals adverse data, the follow-up investigative process inevitably involves providing the individual notice.

We think the procedures we are currently using achieve the notice that the bill aims at in a way that allows matching programs to be operated efficiently and at the same time preserves the privacy rights of the individual. Anything more would probably be unnecessary overkill and we recommend that the wording of the section be amended to make it clear that general notice of specific matches would constitute the kind of notice that the bill calls for. For our part, we will ensure that application forms used by the Federal agencies will be scrutinized for the adequacy of their Privacy Act notices. And, as you know, under the Paperwork Reduction Act, all of these forms must be approved in advance by OMB.

o Section 3 of the bill amends the Privacy Act to require publication of notices of matching programs in the Federal Register 30 days prior to their initiation. It also amends the Privacy Act to put reports on matching programs in the same reporting category as reports on new Privacy Act systems of records.

We would urge that the provision be amended to permit OMB to waive the publication and review time period if the agency can demonstrate that public harm will result from a delay in conducting the match.

o Section 4 of the bill requires that agencies establish Data Integrity Boards to approve matching programs and to carry out some of the review requirements of OMB Circular No. A-130. Since the IG is not a statutory member of this group, this provision would unwisely conflict with his independence and authorities. Moreover, it is not clear that adding another bureaucratic layer to agency level oversight is appropriate.

Instead, we would like to propose an administrative solution that goes somewhat beyond the statutory proposal. Two OMB regulations, OMB Circular Nos. A-123 and A-130 already address aspects of the oversight problem. A-123 charges agency managers to work actively to prevent fraud and waste and to implement the requirements of the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512), especially as related to conducting reviews to uncover weaknesses in internal management control and accounting systems. The Circular requires two kinds of reviews:

- -- The first assesses the risk of fraud, waste and abuse, as well as other losses in program and administrative activities.

- -- The other requires a more detailed review of higher risk areas to find out if needed controls are in place and working.

Reports to the President and Congress are made annually as to whether agency heads have reasonable assurance that controls are in place and working and that list material weaknesses in the controls.

When I sent the circular to the agencies in August, I asked them to "place a particular emphasis in the next few years on preventing unauthorized use of confidential information -- of both manual and automated files and telecommunications. Maintaining privacy for U.S. citizens is an important goal of this Administration."

OMB Circular No. 130 works with A-123. It states the government's policy on information and the technology associated with its creation, maintenance, use and disposition. Appendix I of this Circular contains requirements for agencies' compliance with the Privacy Act, including requirements for many of the reviews that the bill also requires the Data Integrity Boards to conduct.

It is clear to me the two Circulars working together embody the elements of such Data Integrity Boards. Indeed, together they add up to a much more comprehensive review and and reporting arrangement than the bill proposes and one that would have a large privacy dimension. What we need to do, and what I propose that we do, is to better integrate these two regulations and develop a much broader based activity within the agencies than one that is concerned only with computer matching. We intend to incorporate the results of this activity into our annual report to Congress.

o Section 5 of the bill deals with the important subject of verification of data. We strongly support the goal of this section -- to ensure fair treatment of individuals affected by computer matches. In fact, virtually all Federal programs currently afford similar protections, not only in computer matching situations but in all circumstances where individual eligibility for benefits is in question, regardless of the source of information. This duplication of requirements between existing statutes, regulations, and case law is of concern to us because it has the potential to cause conflict and confusion in program operations.

In a typical federally-funded benefit program, client circumstances change frequently and information flows to caseworkers from many sources -- the clients, other programs, State and local agencies, as well as through computer matching programs with Federal sources. These programs routinely verify the information, provide an opportunity to refute, and give notice of an adverse action and right to hearing. A separate requirement, as proposed by this bill, would burden caseworkers with tracking the source of information in case files so that they could comply with two sets of due process rules. To avoid this, we would recommend that the bill affirmatively state what should constitute the minimum protections applicable to all programs, without attempting to write any specifically into law.

We would also point out that the requirement that all information be independently verified, through either the affected individual or a third party, may cause some operational problems. For example, Social Security Administration data on Social Security benefits cannot be independently verified by any third party; an agency using this information would be compelled to verify it by contacting the recipient and this could jeopardize an agency investigation in a criminal case. We recommend that the bill requirement for independent verification be modified to permit agencies to use the data without independent verification in limited situations.

- Section 2(a) of the bill adds a new disclosure exception to the Privacy Act to authorize data sharing without the consent of the record subject when it is done pursuant to a "matching agreement," the terms of which are defined in Section 2(b) of the bill.

While we think that it will be useful to have such a disclosure exception, we think the provision as proposed is overly broad. It will bring within its scope matches that we do not think the drafters intended to cover. Two specific examples come to mind:

-- Matches on individuals made for law enforcement purposes - from systems like the National Driver Register, for example.

-- Internal agency matches for administrative purposes when the "hits" are disclosed outside the agency - for overtime payment, for example.

In each of these cases, (b)(12) would require that the matching agency go through all the agreement, notice and due process steps. We do not think that this is what the drafters intended. We suggest, therefore, that the provision be redrafted to cover only a more narrow category of matching programs.

I want to emphasize that these concerns I've expressed relate primarily to how the bill's provisions would actually be implemented. But, we will have to deal with these concerns effectively if we are to avoid unwarranted damage to an important tool in all of our efforts to reduce fraud, waste and abuse. Again, let me say that we are in agreement about the bill's underlying goal: to improve the efficiency of governmental programs while protecting the privacy rights of our citizens. We look forward to working with you in this important endeavor.

This concludes my statement. I'll take any questions you have.

PREPARED STATEMENT OF JOSEPH F. DELFICO

Mr. Chairman and members of the Committee, we are pleased to appear today to discuss the preliminary results of the work we are doing at your request on the Deficit Reduction Act of 1984 and to provide our views on S.2756, "The Computer Matching and Privacy Protection Act of 1986".

The Deficit Reduction Act of 1984

As you know Section 2651 of the Deficit Reduction Act (herein referred to as DEFRA) requires each state to have an Income and Eligibility Verification System in place by October 1, 1986. Among other requirements, DEFRA requires state agencies responsible for such programs as Aid to Families with Dependent Children, Food Stamp, and Medicaid to use certain federal tax information as a check on the accuracy of income declared by applicants and recipients. In addition to state administered programs, DEFRA authorizes the Supplemental Security Income program which is administered by the Social Security Administration, to access and use, for eligibility verification purposes, unearned income data from the IRS.

Accurate income information is essential to the determination of benefit amounts and to verify applicant and recipient eligibility. Most of the federal tax information to be used in these programs will not come directly from information on individual tax returns. Rather, its source will be the tax reports filed annually with the federal government by employers, banks, insurance companies, and others. These tax reports, among other sources, provide information used routinely by the IRS to verify the accuracy of information reported by taxpayers. DEFRA requires states to obtain earnings and pension data from the Social Security Administration, and unearned income, data such as interest and dividends from the IRS.

GAO's current work for the Committee

In July 1985, you requested that we keep abreast of the federal and state efforts to establish the eligibility verification systems required by DEFRA. You pointed out that this federal-state data exchange would, when fully operational, constitute one of the largest computer matching programs ever authorized by the Congress.

To do the work we reviewed the proposed federal rules, resulting comments, and the final system rules. On June 3, 1986, we sent a questionnaire to all states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands. The questionnaire covered a number of topics but concentrated on the current status of implementation in each state including how each planned to request, receive, and use tax data within the rules established by the federal agencies and the time frames established by DEFRA. To date we have received replies from 53 of the 54 jurisdictions. Today we will summarize selective questionnaire results. Aggregate results of the questionnaire are included in the attachment.

While many states told us of problems they have encountered or anticipate facing in implementing the DEFRA provisions, all but four said they expect to have the required systems and necessary staff in place to request, use for verification purposes, and safeguard tax data by October 1, 1986.

Delay of Automated Systems Development

One reported problem, common to 32 states, is that current automated systems development will be postponed or disrupted for periods of 9 months or longer while those states divert resources to make reprogramming, procedural, and other changes to their existing systems to meet the October 1, 1986 date. Most of these states reported that in the interim they would be operating less than fully efficient systems requiring case workers to do more manual case reviews.

Need for Rule Clarification

A number of states expressed concerns to us about the need for clarification in interpreting and applying DEFRA rules. Questionnaire responses indicated, for example, concerns about the allowable amount of time to process their welfare caseloads. We re-contacted 14 states and found that half had interpreted one rule to mean that beginning October 1, 1986, they had to match their entire welfare caseload with federal tax data and within a thirty day period take action on at least 80 percent of the cases. We sought clarification from the Presidents' Council on Management Improvement who coordinated development of the DEFRA rules, and were told that it was not mandatory for a state to process its entire case load immediately. They said that a state could incrementally process its caseload so long as it matched every recipient at least once during a one year period. Some states told us that this interpretation could make a significant difference in the way the states prepared for implementation.

Safeguarding Data

One area in which nearly all states said they anticipate no problems is in the safeguarding of data. State agencies administering needs-based programs regularly obtain, use, and safeguard personal data during the normal course of their work. Most states replied that their existing systems ensure the security and confidentiality of data and thus they anticipated no problems in meeting the safeguarding standards established by the IRS and the Social Security Administration for their data.

In July 1985, IRS provided guidelines to the states containing procedures to be followed in requesting and safeguarding unearned income tax data. The Social Security Administration on the other hand, did not issue its data access guidelines to the states until July 1986. To date, 39 states have signed data access and safeguarding agreements with the IRS and the rest are expected to sign shortly. Ten states have signed data exchange agreements with the Social Security Administration. To date, 6 states have received tax data from IRS and none have received such data from the Social Security Administration.

State Cost and Benefit Concerns

Most states expressed some concerns about the costs and related benefits to be derived from using tax data to verify income and assets declared by applicants and recipients. Since state agencies administering programs under DEFRA have had virtually no experience using such tax data as interest and dividend data for eligibility verification purposes, we feel it is premature to reach conclusions about state's intitial predictions. However, more accurate estimates of costs and benefits will become available after states begin using tax data, at which time they will be in a better position to make assessments.

To our knowledge, the only documented usage of such tax data occurred in July 1985, when the Social Security Administration obtained and used unearned income data, that is, interest and dividends, to identify errors in the Supplemental Security Income program. Preliminary data from a recent Social Security Administration study indicates net savings of $79 million. The study showed that identified overpayments exceeded--by $68 million--the amount of overpayments which would have been uncovered in the programs' normal re-determination process. That process does not have access to unearned income tax data.

Many of the cases uncovered in that computer match were categorized as recipient non-reporting of interest, dividends, and related principal amounts. For example, in one case a recipient was identified as having received a large interest payment. Further investigation disclosed that several years earlier the recipient had received insurance proceeds of $3 million but had failed to report this event. During a subsequent re-determination the recipient denied the existence of any income or resources. The recipient was overpaid about $7000 in benefits. This case was eventually referred to the HHS Inspector General for fraud investigation. Since the recipient's account was with an out-of-state bank, the match with the IRS data was the only feasible means to detect the unreported income and asset--illustrating the point that there may be no other reliable source for verifying the truth of recipients' declarations that they have no income or assets.

Comments on S.2756

This concludes our remarks on the implementation of Section 2651 of the Deficit Reduction Act. The remainder of my statement provides our views on S.2756 "The Computer Matching and Privacy Protection Act of 1986".

Types of Computer Matches to be Covered

First, you asked our views on the types of matches that should be covered by this bill. We believe distinctions should be made between computer matching to verify eligibility in benefit payment systems, and matching done for such other purposes as law enforcement. In either case, however, the flow and usage of the data used in matching needs to be controlled to protect the privacy of individuals.

We believe that the exchange of data to verify declarations made by applicants and recipients of benefit payment systems can be controlled effectively by the provisions of this bill without hampering the ability of those systems to detect errors.

However, criminal investigations or similar government activities outside of benefit payment system management might be adversely affected by certain bill provisions. Thus we question whether the notification requirements in Sections 2 and 3 of the bill should apply to such agencies as those engaged in law enforcement. Section 2 requires an agreement to notify individuals, and Section 3 requires advance Federal Register notification about upcoming matches. Such notifications could neutralize the effects of law enforcement matches which by their very nature, must be kept confidential. But we also are concerned that law enforcement agencies properly protect information and guard against unwarranted disclosure or abuse of information they gather. To that end, such agencies should have Data Integrity Boards and have their matches and use of such information periodically reviewed by such independent groups as the Boards.

We support extending the bill's provision requiring matching agreements to state agencies administering federally financed benefit payment systems. We take this position because these agencies manage federal programs and have legitimate informational needs to verify declarations made by applicants and recipients. Under DEFRA, states will have primary responsibility for using tax data to verify eligibility for such programs as Aid to Families with Dependent Children, Food Stamps, and Medicaid. States answering our survey believed that the safeguard and independent verification requirements of DEFRA are not administratively onerous so we have reason to believe they could comply relatively easily with the similar provisions of S.2756.

Matching Agreements

You also asked us to comment about the matching agreements required by Section 2 of the bill. Basically we believe that this section is fairly complete, provides information for future audits, and establishes a much needed vehicle for review and oversight of data exchanges and computer matching. Some clarification and redefinition, however, would be helpful.

First, the bill is unclear with respect to whether and how matches using data that may be or may have been disclosed under existing disclosure conditions of subsection (b) of the Privacy Act would require matching agreements. If your intent is to make all matches subject to matching agreements, then you may wish to make Section 2 a separate section of the Privacy Act, rather than including it as another of the Act's disclosure conditions.

Second, you may wish to consider the need for matching agreements to be tailored and adapted to the particular needs of certain agencies such as law enforcement agencies--as discussed earlier.

Third, we question why there is a requirement after an agreement is reached between agencies for 30 days to elapse before data can be disclosed, and why data should not flow once the agreement is signed by both parties. In the case of matches aimed at verifying income such as for welfare programs, the timing of such matches and subsequent verification is important because of the relatively rapid movement of recipients on and off welfare rolls. We recognize, however, that in cases where one agreement covers a series of matches and time may be less critical, our concern about the 30 day waiting period becomes less important.

Section 2 dealing with notifying individuals of matching programs should, we believe, specify the method of notification to be used for benefit payment system matches that can involve large data bases. We believe methods such as individually notifying each affected individual whenever such a match is performed may not be desirable. The costs and time required could possibly negate the benefits of the match.

A clause that could be added to section 2 for benefit payment system matches would require agencies to establish procedures for notifying applicants and later, recipients when benefits are redetermined. Section 2 could state that "all applicants for and recipients of federal financial assistance shall be notified at the time of application and periodially thereafter that the information they provide will be subject to verification using such available information as third party reports of wages, interest and dividends, and payment information from other government agencies". This notification language could be included on application and re-determination forms or along with benefit payment checks as well as verbally explained by caseworkers when they contact applicants or recipients.

Finally, we suggest the addition of a matching agreement provision in Section 2 specifying that "information obtained by a matching agency which pertains to the accuracy or completeness of records, be provided to the source agency". This will assist the source agency in correcting any inaccurate or incomplete data in its data base. It has been our experience that a matching agency gains many insights into the accuracy and completeness of supplied data during the matching process and this could be most helpful to the source agency and to other matching agencies as well.

Data Integrity Boards

We support the idea of establishing Data Integrity Boards in all executive agencies to help ensure compliance with the Privacy Act. Our experience shows that agency privacy officers have limited roles, responsibilities, and resources for ensuring such compliance. We are concerned, however, that the Boards' could become administratively burdensome particularly at some smaller agencies. To help guard against this, we believe the Boards' size, organization, and duties should be consistent with the levels of each agency's data exchange and computer matching activity.

Regarding Section 4 of the bill relating to the Board's reporting requirements, we believe that requiring each board to report to Congress annually might overburden and deluge Congress with the voluminous reports. We suggest that the Boards report only to the Office of Management and Budget, which in turn can compile a consolidated report. This would serve the purpose of informing Congress without needless paperwork increases.

Regarding Section 4 covering the Data Integrity Board's responsibility to receive information on the accuracy and reliability of records, we suggest that the wording be changed as follows: "serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs or front-end eligibility verification programs". This would make the Data Integrity Boards' responsibility for data accuracy consistent with our suggested addition to the bill's matching agreement section --toward the end of assisting source agencies in correcting any inaccurate or incomplete data in their files.

We further suggest that an additional responsibility of the Data Integrity Boards might be publishing notice in the Federal Register as required by Section 3(a)(3). Since the Boards will be focal points within agencies for data exchanges, it seems appropriate that they also should have this responsibility. Related language could be added in Section 4 to cover this.

Verification and Notice Procedures

Your final request was for our views on the verification and notice procedures required by Section 5 of the bill. We endorse the provisions of this section, believing they provide an adequate measure of privacy and due process protection to individuals subject to eligibility tests through matching programs and front-end eligibility verification programs. Because of the errors that may be part of any matching program and the harm that the use of unverified information may cause, we feel strongly that these steps must be taken to protect individual privacy.

This concludes my statement. We would be pleased to respond to any questions you or other Members of the Subcommittee may have.

GAO's Work on the Deficit Reduction Act of 1984

In July 1985, the Chairman, Subcommittee on Oversight of Government Management, Committee on Governmental Affairs, requested GAO to keep abreast of the federal and state efforts to establish income and eligibility verification systems required by Section 265[1] of the Deficit Reduction Act of 1984. At that time, the Chairman pointed out that this federal-state data exchange will, when fully operational, constitute one of the largest computer matching programs ever authorized by the Congress. Accordingly, we were asked to closely monitor the federal and state implementation of the systems mandated by DEFRA. Specifically, we were asked to focus our work on (1) resource, coordination, and procedural issues arising from the dissemination and use of federal information; (2) the state agencies' ability to effectively use and control large amounts of tax data, especially in the areas of verification and confidentiality; and (3) issues relating to the need for effective federal and state oversight of the use of the federal information.

In doing our work, we established contact points with federal and state officials responsible for making system rules and providing and using tax information. We reviewed the proposed federal rules, resulting comments, and the final system rules. Immediately after issuance of the final rules we sent a questionnaire to all states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands.

The questionnaire covered a number of topics but concentrated on the current status of implementation in each state and whether each planned to be in a position to effectively accept and use tax data within the rules established by the federal agencies and the time frames established by DEFRA. To date we have received replies from 53 of the 54 jurisdictions. The following copy of the questionnaire has been annotated to show the responses of the replying states.

PREPARED STATEMENT OF RONALD L. PLESSER

Senator Cohen, members of the Subcommittee: my name is Ronald L. Plesser and I am pleased to accept your kind invitation to testify at these hearings as the official designee of the American Bar Association President, Eugene C. Thomas. It is with unique pleasure that I come to this Subcommittee to strongly support your efforts to enact legislation to establish safeguards for computer matching programs. I am a member of the governing council of the Individual Rights and Responsibilities Section of the ABA. I was the General Counsel of the U.S. Privacy Protection Study Commission and have spent many years working with the Privacy Act. The views I express today are the views of the American Bar Association as adopted at its Annual Meeting during August of this year in New York.

In summary, the policy of the ABA is fully consistent with the provisions of S. 2756, although the legislation does not, on certain points go far enough. There are, in addition, several provisions in S. 2756 which were not considered by the ABA and/or which, thus, has no position. We will be consulting with the Section of Science and Technology and other interested ABA groups on these sections. However, I am here to express ABA support for S. 2756; we look forward to continuing to work with you on the other sections of S. 2756 in order to strengthen our ability to protect individual rights in the field of privacy and computer matching.

During the past three years, the Section of Individual Rights and Responsibilities, through its Privacy Committee and its symposia series on Privacy, Information Policy and Technology has met with key government officials responsible for implementing the federal government's Long Term Matching Program. We have engaged in a serious dialogue about the privacy implications of computer matching. While policy differences remain, a significant consensus has emerged on a number of critical issues which pave the way for a concerted effort to implement a number of reforms. This consensus was developed during the privacy symposium sponsored by our section in Washington, D.C. on October 19, 1985.

We strongly support efforts to curtail waste, fraud and abuse in government benefit programs. However, government officials and privacy advocates are in fundamental agreement that computer matching of data bases containing personal information to detect fraud and abuse in government benefit programs and the growing linkage of different data bases of personal information for purposes of verifying benefit claims, contractor billing, and tax returns, among other purposes, pose significant privacy concerns which must be addressed by Congress. There is also agreement on the basic due process requirements which should govern all matching programs.

Computer Matching of Personal Information

Computer matching involves the use of computers to "run," or compare, one data base of information against another to search for particular similarities or discrepancies between the two. Computer matching does not in and of itself pose privacy issues. What is of concern is computer matching of a data base containing personal information against another data base containing personal information collected for a different purpose. An example: a data base containing personal data on food stamp beneficiaries is run against a data base of customer bank records to find food stamp recipients who may have unreported income which would disqualify them from receiving foods stamps.

Today, federal agencies conduct as many as 200 ongoing matching programs of this kind involving a wide array of government benefit programs from food stamps to medicare. It is being used for other purposes as well, including locating persons who have not registered for the draft and persons who have not paid child support. Matches are being run against state wage reports required of all employers, unemployment compensation records, and as a consequence of the Deficit Reduction Act of 1984, unearned income information from the Internal Revenue Service. See Public Law 98-369 (1984).

Increasingly, many of these data bases are being linked for "front end verification" purposes. Instead of or in addition to matching, a front end verification allows a government agency to verify information provided by a person, for instance, in an application for a government benefit, by querying a large data base containing data from different sources: data files on persons receiving various government benefits, employment and wage information, and at the state level, bank and credit records. If a person can be disqualified at the outset, there is less need to "match" and detect errors after the fact. It is more efficient and in the view of some, less objectionable since the citizen has actual notice of the verification process and may give at least implied consent by seeking a benefit. Moreover, there is no "search" through the records of thousands of persons.

On the other hand, what is developing may be a de facto data base on every citizen in the United States. For example, the Administration is about to come forward with legislation that would, if enacted, extend current matching and verification procedures to a host of programs including Pell grants, guaranteed student loans, veterans benefits, HUD housing assistance, school lunch payments, railroad retirement benefits, health education assistance and nursing student loans. Personal information data from these programs would be added and linked to the needs-based programs such as food stamps and Medicare covered under present law which, as mentioned, includes wage and IRS unearned income data. The Administration is also planning to ask Congress for legislation to establish a Health Insurance Verification System which would require and include information on every citizen's private or public medical insurance plans and records to insure that proper billing and insurance payments take place.

Privacy Issues

There are seven discrete areas where the ABA is concerned that these matching programs impact on privacy issues. I will briefly summarize those concerns.

Fourth Amendment. Many privacy advocates have advanced the argument that computer matching of data bases containing personal information amounts to a general search in violation of the Fourth Amendment since thousands of records may be searched without any evidence that the targets of the search are engaged in criminal activity. But far more intrusive "categorical" searches are sanctioned under current law (e.g. airport scanning of luggage), leaving little possibility that the courts would declare matching unconstitutional. Moreover, since such searches turn on levels of intrusiveness, a legal challenge is likely to fail because the Supreme Court has already declared that citizens have no privacy right in third party records. See United States v. Miller, 96 S. Ct. 1619 (1976).

Finally, it may be persuasively argued that a computer match program does not "search" through thousands of records but only scans and "ignores" records unless preselected record "fields" contain relevant discrepancies. In other words, only records where there are "hits" are searched. Viewed this way, matching may meet an individualized suspicion test. Moreover, as the government moves towards front end verification procedures using linked data bases rather than matching, the general search critique becomes inapplicable since the data base is only queried for particular persons when they apply for benefit programs.

Privacy Act. A more weighty privacy objection is that computer matching of personal data bases and the linking of different data bases of personal information violates the Privacy Act, which requires that personal information collected for one purpose may not be used for a different purpose without notice to the subject of the record and obtaining his or her consent for each use. See Sec. 552 a.(b). Public Law 93-579 (1974) Unfortunately, the Act contains a "routine use" exception to this rule which has been used to justify computer matching of different government data bases. See Sec. 552 a.(7). No successful legal challenge to computer matching has been mounted on Privacy Act grounds. Such a challenge today is moot because Congress has in fact authorized by legislation most of the ongoing matching programs, overriding whatever protection the Privacy Act afforded.

Fair Information Practice Principle. Computer matching and data linkage may not violate current law, but they do violate the fair information practice that personal information collected for one purpose may not be used for another without notice or consent. This principle is embodied in an American Bar Association Resolution adopted in 1979 which states: "There must be a way for an individual to prevent information obtained for one purpose from being used or made available for other purposes without his or her consent." Up to the present, the government has taken the position that any notice requirement is satisfied if a description of proposed matches is published in the Federal Register. This is insufficient notice, and without actual notice that personal information being supplied may be used for other purposes, there is no way to even imply citizen consent to particular computer matches or data linkages.

Due Process. Computer matching has also led to due process violations in some cases. In 1982 the state of Massachusetts matched welfare records against state bank records. In cases where there were "hits" indicating that clients had bank assets, benefits were immediately terminated without fair notice or a hearing. Later it turned out that some "hits" were serious errors. Some persons were identified as having bank accounts who did not. Some account information was out of date. Some citizens had funds which they were legally unable to use (trust funds) or were allowable under welfare rules (burial expense accounts).

Data Security. As more sensitive personal data is accumulated and linked together, privacy rights are threatened by inadequate attention to data security issues. Neither the Executive Branch nor the Congress have developed adequate security measures to protect data bases from unauthorized access.

Data Merging. Data linkage permits the government to query a number of files on citizens. It also paves the way for the possibility of merging data into new data bases which may have significant adverse impacts on privacy. For example, recent statutes have authorized the IRS to deduct debts owed the government from IRS tax refunds. To implement these laws, the IRS is proposing to establish a master debtor file to match against IRS returns.

Fundamental Privacy Rights. As files are linked, the overarching issue is one of privacy and autonomy of citizens as against the government's power and authority to accumulate massive data bases on citizens. Substantive limits on data linkage have to be established. At some point, privacy and autonomy outweigh government efficiency. Substantive barriers have to be created to prevent the government from linking sensitive data on citizens such as personal tax information, medical records, census data, and data on citizens' political and religious beliefs.

Policy Recommendations

Computer matching and data linkage programs must be overseen by the Congress and such programs must be authorized by legislation which strikes a proper balance between governmental purposes and individual privacy and autonomy and which are consistent with established fair information practices.

The ABA recommends the implementation of this general principle through enactment of legislation addressing the six areas identified in the ABA's resolution:

> BE IT RESOLVED, that the American Bar Association supports enactment of legislation to amend the federal Privacy Act of 1974 and other legislation to: (1) prohibit the non-consensual use of income tax, census, political activity, religious affiliation and similarly sensitive data files for the purpose of verifying the eligilibity of citizens for government benefit programs; (2) require specific notice to applicants that personal information provided by an applicant may

> be compared with other personal information about the applicant in specified government and private data bases to verify the accuracy of the data provided; (3) require a government agency to obtain independent specific verification of any computerized data comparison before a government benefit is terminated or denied; (4) afford each benefit applicant due process, including notice of the right to correct and complete a government record and a fair hearing at which an applicant or beneficiary may contest an agency decision to terminate or deny a benefit on the basis of information obtained from computerized data comparisons independently verified; (5) prohibit the merging of personal data supplied by one agency for verification purposes with the personal information data of another agency, and to require that any such file temporarily created for data verification purposes be destroyed upon completion of the matching operations; (6) establish strict limits on access to computerized personal data files to insure they are not used for different or incompatible purposes or accessed by persons without proper authority.

Part one of our policy would bolster current policy and practice. To use IRS and census files for government eligibility verification programs would violate current prohibitions in federal law. In 1984 Congress authorized the use of unearned income files of the IRS for computer matching programs by amending the law. In doing so, we believe the Congress paid insufficient attention to the public interest in citizen privacy and personal autonomy involved in making more and increasingly more sensitive information available for matching and verification programs. The American Bar Association opposes further "exceptions" to current statutory prohibitions on the use of sensitive files.

Part two of our resolution calls on the government to give citizens actual notice that personal information may be used for computer matching programs. For example, federal employees would be given notice when they applied for a job that the information supplied may be matched against food stamp files, AFDC, and student loan programs. Currently, the government meets the notice requirement under the Privacy Act by publishing a proposed computer matching program in the federal register. This is inadequate notice. Under the Deficit Reduction Act, the Congress established actual notice requirements for some computer matching programs. If implemented, the ABA policy would require notice across the board. Since notice that information may be checked would deter fraud, the government should not object. The value from a fair information practice point of view is that citizens should know how information collected about them will be used when they supply that information.

Part three of our resolution is current government policy and is a requirement for some programs by statute because of the Deficit Reduction Act. This avoids termination or denial of benefits solely on the basis of a "computer match" which may turn out to be a "computer error."

Part four of our policy is also current government policy but it can be strengthened through legislation. For example, applicants for benefits often do not know of their right to correct a file. Every citizen knows the difficulty of arguing with a computerized bill which is in error. Citizens need to know their rights and be able to correct computer files either directly (by computer terminal) or with government assistance. The ABA can use this policy to work for innovative changes, such as more explicit notice, giving citizens computerized access to their files for correction and completion purposes, requiring agencies to assist citizens in correcting and completing files.

Part five of our policy addresses the danger of the development of de facto national data files on every citizen. Government officials are in complete agreement that such files should not be created. A statutory prohibition would constitute a significant step forward.

Finally, part six of our policy is of crucial importance. While data security is a government concern, it is not a government priority. Few resources are devoted to data security procedures or oversight over who has access to these expanding data files. The ABA urges that Congress make this a priority.

Conclusion

We strongly agree that the government must embark on vigorous programs to minimize waste, fraud and abuse in benefit programs. Adoption by the Congress of these recommendations -- many of which are in S. 2756 -- would help insure a proper balance between such efforts and the need to protect legitimate privacy and due process of our citizens. Historically, it is respect for the privacy of the individual which has distinguished our society from totalitarian regimes.

PREPARED STATEMENT OF JERRY J. BERMAN

Mr. Chairman and Members of the Committee:

Introduction:

On behalf of the American Civil Liberties Union, I welcome this opportunity to testify today on S. 2756, "the Computer Matching and Privacy Protection Act of 1986." As you know, the American Civil Liberties Union is a nonpartisan organization of over 250,000 members dedicated to the defense and enhancement of civil liberties guaranteed by the Bill of Rights.

At the outset, I want to commend you, Mr. Chairman, for your leadership in calling public attention to the privacy issues posed by computer matching and data linkage and for introducing this significant privacy initiative. I also want to commend Senator Carl Levin for joining with you in sponsoring this legislation.

We consider enactment of legislation along the lines of S. 2756 a matter of high priority. Computer matching, despite its adverse impact on information privacy rights, has been institutionalized government wide. Rather than continuing to call for a ban on matching or continuing to suggest that it is subject to constitutional or legal challenge under present law, we must recognize that matching and verification programs are here to stay and unfortunately are lawful under current statutes and judicial precedent. We must seek to vindicate privacy and due process rights through legislation such as S. 2756.

While supporting S. 2756, we want to make it clear at the outset that it is not as far reaching as we would like nor do we believe it is responsive to the fundamental civil liberties issue posed by matching and verification programs---the development of what the recently published Office of Technology Assessment study, Electronic Record Systems and Individual Privacy (hereinafter OTA Privacy Study) terms "the creation of a *de facto* national database containing personal information on most Americans."

Nevertheless, if we want to achieve reforms, we must work for legislation which can command broad support from the Congress and the Administration. Our goal is not a "model" bill. It is to change the law. S. 2756 in our view is in the realm of the possible and a significant step in the right direction.

In this regard, we note that over the past year, privacy advocates and government officials have discussed computer matching and verification issues on a number of occasions. Our Project on Privacy and Technology, the Individual Rights Section of the ABA, and the Office of Technology Assessment have all provided forums for a discussion of different views and a search for common ground. We believe that S. 2756 sets out a legal framework for computer matching and verification programs that incorporates---subject of course to some modification and interpretation---a common set of principles which appeared to emerge from these discussions. S. 2756 may thus garner the broad support necessary for enactment.

In our testimony today, we explain why we have come to support S. 2756, discuss what we believe are its most important provisions, and recommend certain modifications. We also state our more fundamental concern about the growth of a "de facto national database" and the need to address this issue over the coming years. Because S. 2756 has only recently been introduced and will be acted on in the next Congress, we expect to present additional comments and suggested amendments when this legislation is taken up next year.

The Unchecked Growth of Computer Matching:

Since the implementation of Project Match by the Carter Administration in 1977, the American Civil Liberties Union and other privacy advocates have criticized computer matching as violative of the privacy and due process rights of citizens. In testimony before this Committee in 1982, we attacked matching programs as "general searches" barred by the Fourth Amendment and a violation of the Privacy Act of 1974 which prohibits the use of personal information/records collected for one purpose from being used for a different purpose without notice to and the consent of persons who are the subject of matched records.

Despite this criticism, the use of computer matching by federal and state government agencies to detect fraud and abuse in government benefit programs and for law enforcement purposes has grown enormously. According to the OTA Privacy Study, there are as many as 110 ongoing federal matching programs today. From 1980 through 1985, 553 separate matches have been conducted. Since 1980, the number of computer matches has nearly tripled. A new federal matching program notice appears almost weekly in the Federal Register.

The growth of computer matching is not difficult to explain. Government officials believe it is an effective tool for detecting fraud and abuse in government programs and increasingly useful in law enforcement investigations. The Administration, with support from the Congress, is committed to reducing fraud and abuse in all benefit programs seemingly without regard for privacy impacts. Whatever technological hurdles existed when matching programs were initiated, officials have overcome most of them and sophisticated computer hardware and software is making even more complicated matches possible and at lower cost.

Most important, computer matching is growing unchecked because there are no serious legal barriers to matching despite criticism that matching violates individual privacy. In a "Focus Paper on Computer Matching" prepared by our Project on Privacy and Technology and appended to this testimony, there is a detailed explanation why matching is legal today. Let me briefly summarize our view of the legal issues.

First: While we have argued that computer scanning through thousands of records with no individualized suspicion of wrongdoing is a "general search" violative of the Fourth Amendment, there is no possibility of winning such a case based on current Supreme Court precedents. A number of categorical searches (e.g. INS checkpoint searches at the border) have been upheld by the Supreme Court even when recognized privacy interests are involved. Since the Court unfortunately has not recognized a protectable privacy interest in personal information held by third parties, a challenge to computer matching on constitutional grounds is even more problematic. Moreover, it is not at all clear that machine scanning through records programmed to search for certain preselected matches of data fields (e.g. name or common social security number in two sets of files) rises to the level of a general search.

Second: While some have argued that computer matching violates the basic principle that a citizen is innocent until proven guilty when benefits are denied on the basis of a mere "hit", the validity of the argument turns on the denial of benefits without further investigation by the matching agency. Since the celebrated 1982 bank match in Massachusetts where recipients' benefits were wrongfully terminated in many cases on the basis of "hits" generated by comparing welfare records with state bank records, agency officials claim they have instituted independent verification procedures before suspending or terminating benefits to avoid such unjustifiable results. If this is the case, the general claim that computer matching violates a presumption of innocence can not be used to attack all matching programs per se.

Third: The most solid ground for attacking computer matching is that these comparisons of different records violate the due process and informational privacy rights incorporated in the Privacy Act of 1974. The drafters of the Privacy Act recognized that we live in a society today which increasingly requires citizens to turn over personal information to government and that to protect privacy required the establishment of a protected privacy right in those records. The drafters also foresaw the coming of an advanced computer age and the need to institute fair information practices to govern the use, exchange, and disclosure of personal information made possible by computerization.

Under the Act, personal information collected for one purpose is prohibited from being used for another different purpose without giving the subject of the record notice and obtaining his or her consent. This provision appears to bar computer matching. In fact, Project Match, the first federal matching program, was debated within the government on these terms. Some officials argued that to match federal employee records with welfare records was illegal under the Act without notice and consent because they were not collected for detecting welfare fraud. Although Project Match and then computer matching in general went forward, we believe and continue to believe matching violates the Act and basic due process rights of citizens.

Unfortunately, as you know, computer matching has been justified under the "routine use" exemption to the Privacy Act and notice to record subjects has been deemed satisfied by publication of a matching program in the Federal Register, a result contrary to the basic intent and purposes of the Privacy Act. However, because the Act does not provide for injunctive relief and provides a civil remedy only when actual damages can be proved, its stated protections are in effect unenforcable. Intangible harms, such as invasion of privacy, require statutory damages like those provided under federal wiretap statutes in order to be vindicated.

Fourth: Even if computer matching violated the Privacy Act, Congress, in a number of statutes, has authorized computer matching and verification programs. Matches covering all need-based programs were essentially reauthorized, including new authority to match against heretofore confidential unearned income records of the IRS, in the Deficit Reduction Act of 1984. Legislation to establish matching and verification procedures for other grant programs (the Payment Integrity Act) is expected to be introduced by the Administration in the near future.

Fifth: Administrative limits or controls on computer matching have been watered down or hardly exist. In 1982 the Carter Administration requirement that computer matching must be cost-justified was eliminated. Oversight over matching proposals or matching program results is almost nonexistent according to the OTA Privacy Study and a Report by the Information Subcommittee of the House Government Operations Committee.

Support for S. 2756

In the face of this legal privacy vacuum, S. 2756 is necessary legislation. It is also balanced legislation and deserves to be enacted. On the one hand, it authorizes computer matching and frontend verification programs which in fact already are routinely conducted by government agencies. On the other hand, it recognizes that matching and verification programs are not mere "auditing" techniques but uses of personal information which affect privacy and due process rights and need to be conducted and overseen with due regard for these rights of citizens. It incorporates "fair information practices" as originally intended by the drafters of the 1974 Privacy Act.

S. 2756 is hardly radical legislation. Many of its provisions (matching agreements, independent verification, and oversight requirements) are already set forth in government regulations. By putting these requirements in statute, however, it insures that they will be taken seriously by all agencies. Other provisions establishing information security procedures, protecting against redisclosure, prohibiting the merging of matching data and requiring information destruction schedules are requirements which officials have discussed with us as current practice and essential privacy protections. Many of these requirements are included in the final regulations on DEFRA issued in February of this year.

New requirements which enhance due process guarantees, such as adequate notice to citizens of the fact that information will be exchanged or verified and prohibiting adverse actions against individuals until information is independently verified or a hearing held, are both reasonable and necessary due process guarantees.

Below we consider some of the most important features of the legislation and some suggested modifications.

Section 2. Matching Agreements

The importance of the bill's detailed matching agreements serves a number of important functions. As structured in the bill, the matching agreements require agencies to articulate their reasons both legal and programatic for establishing a matching or verification program and to set forth how they plan to protect due process and privacy rights.

With publication in the Federal Register, the level of detail also makes agency, congressional, and public oversight over computer matching and front-end verification possible. For example, today there is no way to tell from a federal register notice of a computer matching program the level of intrusiveness involved in a particular match or what steps are being taken to protect data from unauthorized access. Requiring publication of the number of data elements, number of records involved, notice and destruction procedures, and other security safeguards will allow the agencies, Data Protection Boards, Congress, and the public to understand the ramifications of a program and make meaningful suggestions for modification and change.

We note that matching agreements must only be entered into between various government agencies. We believe matching agreements should also cover agreements between federal agencies and private source entities such as banks and credit companies.

TRW and other credit companies today are exchanging bad debt information with federal agencies. In 1982 this Committee learned that the IRS was attempting to buy data compiled by marketing agencies to detect tax evaders. These exchanges, if they occur, should be governed by matching agreements and would be covered under the Statute by amending the definition of "non-Federal matching entity" to cover private source entities.

Sec.2(1) Justification

To evaluate computer matching and verification programs, we would urge that justification include documentation of past results (e.g. fraud detected) if it is a recurring program or anticipated results (e.g. projected hits) if it is a new program.

In our view the cost/benefit requirement contained in the original 1979 computer matching regulations offered scant protection for privacy rights. Such measurements are always subject to conflicting interpretation and the agencies will usually be able to make a case for cost effectiveness. Nevertheless, the inability of the government to come up with solid numbers on the value of particular matching programs (see OTA Privacy Study) would be rectified by making this a part of the justification requirement and may eventually lead to the termination of some matching programs on cost effectiveness grounds.

Sec. 2(2) Data Elements and Number of Records

As mentioned, this is a particularly important criteria for privacy oversight. It allows a judgment about the intrusiveness and scope of a particular matching program.

Sec. 2(3) Notice

This is one of the most important due process provisions in the proposed statute. We hope that legislative history or the statute itself will make clear that notice must be actual notice to the subject of the record on how personal information supplied to the government will be used, exchanged or verified.

Notice today is publication in the Federal Register. Since most citizens do not read the federal register, this form of notice is simply unacceptable. Notice should be on the application form and spelled out in plain language. Today, when notice appears on a form, it is often unintelligible. For example, here is how notice is handled on a Veterans Administration form:

> "The information submitted may be disclosed outside the Veterans Administration (VA) only as permitted by law, including the routine uses identified in VA system of records 58VA 21/22/28, Compensation, Pension, Education and Rehabilitation Records--VA published in the Federal Register."

In addition, some agencies disclose that collateral sources will be contacted. Others do not. Uniform disclosure by all agencies should be a part of the notice requirement.

Notice should also advise citizens (pursuant to Section 5 and the Privacy Act in general) that they have a right to correct information and that benefits may not be denied or terminated unless independently verified and subject to a citizen's right to a hearing. Citizens are rarely informed by government agencies of their right to see and correct records. Legislative history should also suggest that agencies consider the possibility of developing means by which citizens can see and correct their records by computerized means.

Although we would also require actual consent to any exchange of information, we know that can not be achieved in this legislation. However, actual notice at least makes implied consent to record exchange or verification a meaningful reality when a citizen applies for and accepts a government benefit.

This due process requirement may pose new burdens for government agencies. However, we think they should embrace this change. From an agency view, clear notice that information will be verified and how will deter citizens from supplying inaccurate or false information knowing that it will be detected. Thus, notice serves the government goal of reducing fraud and abuse in government benefit programs.

Sec.2(4)Verification & Verification Under Section 5

Verification procedures must be specified in all matching agreements under (4) of this section. Under a separate Section 5, the statute would provide that no individual's benefit may be suspended or terminated without independent human verification and without providing a citizen an opportunity to refute (we would add correct) information produced by a matching or front end verification program including a right to a hearing. We discuss this section here.

In our view, these requirements, together with actual notice, constitute the core due process protections afforded by the proposed legislation. While government agencies have instituted some independent verification procedures, these sections spell out what Congress intends by verification and makes it a matter of fundamental fairness.

Placing this requirement in statute and applying it to all information which may adversely affect benefit rights is essential. We note that in issuing regulations for DEFRA, some affected agencies read the verification requirements only to mean that they have to verify IRS unearned income data. These sections will make it clear that Congress intends all wage, income, and asset information to be verified.

- Independent human verification of computer matches is essential to protect due process and the presumption of innocence. No benefit should be suspended or terminated without such verification.

Computer databases are replete with incomplete, false, and inaccurate data. For example, under DEFRA, benefit applications are to be checked against IRS unearned income records. The need for such verification has been amply documented. In recent testimony before the House, John Finch of the General Accounting Office revealed that faulty software used by a number of banks to report unearned income to the IRS led to inaccurate IRS reporting "affecting approximately one million taxpayers." According to some state officials we have talked with, significant error rates can also occur in other wage and income data.

We would also urge that matching agreements under 2(4) and Section 5 require reasonable time limits for verifying information. Long delays may adversely affect citizens if they must wait for verification to receive benefits. Under 5, we would recommend that if verification time limits are exceeded through no fault of an applicant, he or she should be presumed qualified and receive benefits pending a final determination.

Finally, independent verification procedures must not be overly intrusive. The statutory language authorizing verification from "third party sources" is subject to broad interpretation (e.g. employee or neighbor interviews) and should be limited to collateral sources.

Sec.2 (5)(6)(7)(8)(9)Privacy Protections

The remaining requirements for matching agreements are designed to protect privacy of records involved in computer matching and verification programs. It is essential that records be protected against unauthorized disclosure or redisclosure and that information used in matching programs is returned to the source agency or destroyed and never merged into new cumulative data files.

In the age of the microcomputer and with the move toward on-line access, careful procedures must be designed and adequate oversight resources devoted to prevent unauthorized access and use of sensitive personal information. In discussing the implementation of DEFRA with federal and state officials, many expressed concern that personal data has been made increasingly vulnerable and that adequate resources are not being devoted to insuring data protection. One necessary element in moving toward protection is the proposed creation of Data Integrity Boards under Section 4 of the legislation.

Section 4. Data Integrity Board

According to the OTA Privacy Study and a Report by the Information Subcommittee of House Government Operations, oversight over matching and verification programs is almost non-existent. The statutory creation of strong Data Integrity Boards in every matching agency would rectify this problem by requiring systematic oversight over these programs. Without tough agency oversight, this Act may never be enforced in an effective way. The failure of the 1974 Privacy Act is due in large measure to the fact that provisions which would have established an overall privacy oversight board were eliminated before final passage.

To insure Board oversight and also to permit more effective Congressional and public oversight, we would urge that the Boards be required to report any agency actions which violate the terms of a matching agreement or which in the opinion of a Board adversely affect privacy or due process rights.

Sanctions under Section 5

Section 5 (c) provides that agencies may not disclose reco if there is "reason to believe" that matching agreement and other requirements are not being followed. A similar sanction governs the FBI's National Crime Information Center which bars federal exchange of records with police agencies who fail to maintain accurate and complete records. It is never used because of overriding law enforcement interests in continuing to exchange records. We doubt whether it will prove to be an effective sanction in the context of matching and verification programs for similar reasons. "Mistakes" will be rectified. Exchanges will continue.

We would recommend an amendment to the statutory tort remedy under the Privacy Act that would allow citizens to recover statutory damages if records are exchanged or disclosed in willful disregard of requirements set forth in matching agreements or in violation of section 5. As I stated earlier, statutory damages are necessary when intangible harms such as invasion of privacy occur and such a remedy is incorporated in federal wiretap statutes and has been proposed as an amendment to the Federal Tort Claims Act in long-pending legislation which would establish government rather than employee liability for constitutional torts.

A De Facto National Data File on Citizens

At the outset of my testimony, I indicated that the ACLU supports S. 2756 because it would enhance privacy and due process protections in the conduct of computer matching and front-end verification programs. I stated, however, that S. 2756 does not address the more fundamental civil liberties problem of the creation of a "de facto national data file" on every American. Let me explain my position.

S. 2756 will not halt but only control computer matching and front-end verification programs such as instituted under the Deficit Reduction Act of 1984. If the statute is enacted, it will afford citizens more due process. But computer matching and verification programs will continue to expand.

As you know, the current government trend is to increase front-end verification of applicant information for all government benefit programs. Front-end verification reduces benefit payment "errors" by detecting non-eligibility before rather than after a citizen receives benefits. Some argue that it also constitutes a lesser intrusion on citizen privacy because it constitutes a search through a particular citizen's file rather than a "general search" through all files. I disagree.

The goal of front-end verification is to achieve quick and accurate benefit determinations. While such determinations may save taxpayers money and serve a citizen's interest in obtaining benefits as soon as possible, they require systems which permit rapid access to more complete and accurate information.

In establishing the Income Eligibility Verification System (IEVS), Congress, in the Deficit Reduction Act of 1984, authorized the use of social security numbers for all need-based programs to make accurate identification of applicants and to permit computer retrieval of data on applicants from a number of different program databases which potentially contain information on applicants and from databases containing wage, pension, unemployment insurance, and other income data, including unearned income from IRS files.

Congress also called for the development of standard formats for databases for a number of programs to facilitate rapid exchange of information. While computerization of all files was not mandated, DEFRA regulation statements and verification time limits set forth in the regulations encourage computerization and in the future, on-line access to information through the employment of computer networking capabilities. The end result, of course, is the "de facto national database" described in the OTA Privacy Study.

As you know, in the 1960's, the Johnson Administration proposed the creation of a central file on every citizen containing social security, income, census, and other sensitive personal information to serve the needs of the welfare state. The idea of a central data file on every citizen was roundly condemned as "Big Brother" government and a threat to privacy and citizen autonomy. The plan was abandoned.

IEVS and its progeny (the Administration will propose legislation to extend IEVS to more programs covering more citizens with more extensive data) make such a data file on most citizens a modern reality. The file does not have to be stored in one mainframe at a central agency. With social security number as identification, common formats, and on-line access, enormous amounts of data may be assembled instantly on any citizen by computer from "decentralized" files.

S. 2756 may make this developing national database more secure, more visible, more subject to oversight. But S. 2756 contains no substantive limits on what files or data may be linked together. With no "bright red line" drawn in law, data linkages will expand. For example, the IEVS system will grow. New programs and data fields will be added. Eventually the system will feature on-line access by federal and state agencies. In the future, the FBI may want access to IEVS for law enforcement or intelligence purposes. Certainly, INS will want access to IEVS to detect illegal aliens. IRS may want to verify income tax returns through the system and pressure will mount to add more IRS data to the system for verification purposes. IEVS is only one of many possible national databases.

I submit that we will pay a significant civil liberties price for developing such sophisticated means for compiling, sharing, and exchanging personal information. Privacy is one value at stake. More fundamentally, and I mean no pun, our sense of individual liberty is on the line.

Information which could be lost in a file drawer ten years ago will now be capable of rapid search and retrieval. Immutable records will impact on how we behave. It will make us more cautious, more conforming, more worried about deviation or dissent. Deviation means a potential discrepancy and discrepancy will call attention to us. The sense that Americans have---as old as the frontier---that if they make a mistake or do something wrong, they can begin again may be ending for all time in today's computer society. If we move West today, all an agency has to do is dial back East and a file follows you.

It is time to begin to pay attention to this development and begin to devise ways to draw limits on this system. The late Senator Sam Ervin put it best:

> "These new sciences have accorded those who control government increased power to discover and record immutably the activities, thoughts, and philosophy of an individual at any given moment of life. That picture of the person is recorded forever, no matter how the person may change as time goes on. Every person's past thus becomes an inescapable part of his present and future.....Unless new controls are enacted, new legislative remedies are provided and unless federal officials can be persuaded to exercise more political self control, this country will not reap the blessings of man's creative spirit which is reflected in computer technology."

S. 2756 will help to focus attention on the issue by enhancing congressional and public oversight on matching and data linkage.

We would also recommend a change in the "routine use" exemption, as recommended by the American Bar Association, that would require express congressional authorization for matching any records which currently are not routinely used for this purpose. An explicit purpose of the amendment would be to require congress to weigh the privacy and civil liberties ramifications of authorizing their use for such purposes. Along with the American Bar Association, we would also recommend an express prohibition on use of 1040 information, political affiliation, race, and other sensitive information in matching or verification programs.

Conclusion

S. 2756 is a major privacy initiative. It will resolve some pressing privacy and due process problems posed by computer matching. In a few years hence, when the matching and verification agreements are drawn up and oversight mechanisms in place, this legislation may also make clear whether further, more fundamental reforms may be necessary.

Again, we thank you for this opportunity to testify today on this important legislation.

9/15/86
cmcohen.tes
pc #2
c:\jerry

STATEMENT OF PRISCILLA M. REGAN
ANALYST, COMMUNICATION AND INFORMATION TECHNOLOGIES PROGRAM
OFFICE OF TECHOLOGY ASSESSMENT
U.S. CONGRESS

BEFORE A HEARING OF THE

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT
COMMITTEE ON GOVERNMENTAL AFFAIRS
U.S. SENATE

Electronic Record Systems and Individual Privacy

September 16, 1986

Mr. Chairman and Members:

Thank you very much for the opportunity to appear before your Subcommittee this morning. Today, we would like to discuss the findings of OTA's report on Electronic Record Systems and Individual Privacy in the context of S.2756, the Computer Matching and Privacy Protection Act of 1986. The report is part of a larger study of the effects of new applications of information technology by the Federal Government, particularly their effects on civil liberties and congressional oversight. The study was requested by the Senate Committee on Governmental Affairs and by the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary.

The OTA report reached three general conclusions:

- new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves;
- there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with the Privacy Act and related OMB guidelines; and
- neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved.

My testimony will address each of these conclusions with respect to computer matching and computer-assisted front-end verification, the subjects of S.2756. However, other problems identified in the OTA report -- such as Federal use of computer profiling, agency use of microcomputers in processing personal information, and agency access to IRS files and files containing sensitive information -- are still in need of congressional consideration.

I will also discuss a number of policy options that OTA identified for congressional consideration, including institutional adjustments to improve oversight and other actions to address specific problems.

Technology and the Privacy Act of 1974

Congress passed the Privacy Act of 1974 to provide individuals with safeguards against invasions of their personal privacy. The act required Federal agencies to meet specified Fair Information Principles and granted individuals new rights with respect to their records held by Federal agencies. Overall, OTA concluded that Federal use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act. In the 12 years since the act was passed, at least two generations of information technology have become available to Federal agencies, including microcomputers, computer networks, on-line data communications, and electronic record searches (such as computer matching, computer-assisted front-end verification, and computer profiling).

These technological advances have opened up new opportunities for improving: 1) the efficiency of government recordkeeping; 2) the detection and prevention of fraud, waste, and abuse; and 3) law enforcement investigations. At the same time, the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. These expanded opportunities make the completeness, accuracy, and relevance of information even more important than in the past. Additionally, this expanded access and use make it nearly impossible for individuals to learn about, let alone seek redress for, misuse of their records by Federal agencies.

As addressed in our report, computer matching presents a good example of the conflicts between the Privacy Act protections and new uses of information technology. Computer matching involves the comparison of two or more sets or systems of computerized records to search for individuals who may be included in more than one file. While not specifically prohibited by the Privacy Act, computer matching would appear to be discouraged by the act's requirement that information collected for one purpose not be used for another purpose without the consent of the individual. There are, however, exceptions to this requirement. One exception is for a "routine use", defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" [sec. a(7)]. Under the 1979 and 1982 Office of Management and Budget (OMB) Matching Guidelines, matching can be considered a routine use. Therefore, individual consent is not required; instead, notice of a proposed match must appear in the Federal Register. Many have questioned the adequacy of such notice as a means of informing individuals, as the vast majority of individuals do not read the Federal Register.

S.2756 contains a number of provisions -- including those for notice, independent verification, and opportunity to refute -- that address the lack of effective notice to individuals whose records are being used in a match and individuals against whom adverse action may be taken as a result of a match. S.2756 also requires a matching agency and a source agency to enter into a written agreement 30 days prior to the match. The written agreements are to specify "that individuals whose records are matched will be notified of such matching program or front-end eligibility verification program and the procedures for providing such notice" [sec. 2(c)(3)]. S.2756 also would make it a statutory requirement to place notice of both matching programs and front-end eligibility programs in the Federal Register 30 days prior to conducting such programs.

The Privacy Act also requires agencies to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs" [sec. e(2)]. In computer matching, information that will be used to determine whether benefits should be terminated, decreased, or increased is collected from third parties -- not from the individual. Such third-party collection increases the possibility that inaccurate or incomplete information will be used. OTA found that some means to verify information is thus important.

S.2756 addresses this finding by requiring that:

> no matching agency or non-Federal matching entity may deny, terminate, suspend, or reduce any Federal financial assistance to such individual, or take other adverse action against such individual as a result of information produced by such programs, until such agency or entity has independently verified such information. Such independent verification may be from third-party sources or the individuals whose records are matched. [sec. 5(a)]

Moreover, S.2756 would require an agency to give the individual an opportunity to refute information produced by a matching program prior to an adverse action. This requirement ensures that an individual will be informed prior to an adverse action and will have an opportunity to present reasons why such an action should not occur.

Similar conflicts with the Privacy Act principles of information collection and use exist in front-end verification programs of Federal agencies. Front-end verification is used to certify the accuracy and completeness of information provided by an applicant by checking it against similar information held in an existing database, generally of a third party. The use of computer-assisted front-end verification dramatically changes the scale and speed of record exchanges in ways that make it virtually impossible for individuals to monitor how their personal information is being used.

The provisions in S.2756 for notice, independent verification, and an opportunity to refute, discussed above, would also apply to front-end verification programs. Thus, S.2756 gives individuals new means to monitor such uses of personal information.

The technological requisites for computer-assisted front-end verification lead to the on-line connection of individual databases, e.g., the IRS's Debtor Master File and the State Income Eligibility Verification Systems. In effect, these linkages create a de facto national database covering nearly all Americans. Although such a database was not specifically prohibited in the Privacy Act, debate and disapproval of proposals for a Federal Data Center in the late 1960s were factors that contributed to enactment of the Privacy Act. S.2756 does not address the national database issue. It is important that Congress not lose sight of the larger picture -- the creation of a de facto national database containing information on most Americans and use of the social security number as a de facto national identifier -- of which computer matching and front-end verification are parts.

Oversight of New Technology Applications

Under the Privacy Act, each agency is given responsibility for its own implementation of the act and OMB is assigned responsibility for executive oversight of the act. Criticisms of OMB's oversight have been well documented in prior studies by the Privacy Protection Study Commission (1977), the U.S. General Accounting Office (1978), and the House Committee on Government Operations (1975 and 1983). Among other concerns, these studies noted a lack of information concerning the activities of Federal agencies with respect to personal information. Given that, OTA conducted a survey of 13 cabinet departments and 20 selected independent agencies. OTA found the following:

- The quality (completeness and accuracy) of most Privacy Act record systems is unknown even to the agencies themselves; only about 13 percent of the record systems are audited for record quality. The limited evidence suggests that quality varies widely.
- Even though the Federal inventory of microcomputers has increased from a few thousand in 1980 to over 100,000 in 1985, very few agencies (about 8 percent) have revised privacy guidelines with respect to microcomputers.
- In most Federal agencies, the number of staff assigned to Privacy Act implementation is limited; of 100 agency components responding to this question, 33 reported less than 1 person per agency assigned to privacy and 34 reported 1 person.
- Eleven cabinet-level departments and 4 independent agencies reported conducting 110 matching programs with a total of approximately 700 matches from 1980 to April 1985.
- In the 5 years from 1980 to 1984, the number of computer matches nearly tripled.
- In only 20 percent of the matches were agencies able to provide information on the number of records matched, number of hits, and percent of hits verified. Despite this low response, the number of separate records used in the reported matching programs totaled over 2 billion; the total number of records matched was reported to be over 7 billion due to multiple matches of the same records.
- Only two agencies -- the Bureau of Indian Affairs in the Department of the Interior and the Veterans Administration -- reported the use of computer-assisted front-end verification.

In analyzing the survey results and after discussions with officials from a number of Federal agencies, OTA concluded that there are few internal agency checks on computer matching and front-end verification programs. Program personnel appear to have substantial discretion in deciding whether or not to use these applications as audit techniques or as means to detect fraud, waste, and abuse. The Inspector General's Office may be involved in planning a computer match or front-end verification; and the General Counsel's Office and the Privacy Act officer may be involved. But it appears that there are no agency or general policy guidelines regarding what types of information should be used, matched against which records of what other agencies, and for what purposes.

The written agreements between matching agency and source agency that S.2756 proposes would help to rectify the difficulties with lack of internal agency control over matching. The inclusion in these agreements of the justification, purpose, and legal authority of the match, the records that will be used, the means of notice and verification, and safeguards to ensure security of the records are all important in enabling an agency to check on program activities. Additionally, it is important for accountability purposes that the written agreements will be approved by the agencies' Data Integrity Boards that S.2756 would require each agency to establish. It is likewise important that these Boards would also review all recurring matching programs.

With respect to external oversight OMB has developed a number of procedural guidelines, most notably the 1979 OMB Guidance to Agencies on Conducting Automated Matching Programs and the 1982 Revised Supplementary Guidance for Conducting Matching Programs. The purpose of these Guidelines was "to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy." In order to achieve this, the Guidelines rely primarily on placing notice of each match in the Federal Register. The 1979 Guidelines provided for a 30-day period for public comment and advance notice to Congress; the

1982 Guidelines dropped these provisions, as well as the requirement for a cost-benefit analysis. OMB and the President's Council on Integrity and Efficiency have also developed a Model Control System for Conducting Computer Matching Projects Involving Individual Privacy Data (1983); however, agencies are not required to follow the Model Control System, or to report to OMB on which procedures were followed. In late 1983, OMB developed a Computer Match Checklist that is supposed to be on file for review by OMB, GAO, or other Federal entities. The Checklist is to include information on notification, number of individuals whose records are to be matched, contractor involvement, and date on which a cost-benefit analysis of the match will be available.

Whether or not there are sufficient procedural guidelines for computer matching, OTA concluded that there is no oversight of agency compliance with these guidelines. In effect, the guidelines could be ignored. OMB has adopted a very passive role, as is evidenced by its lack of information on the scope and magnitude of computer matching, the quality of the personal information used, and the results and cost-effectiveness of computer matching. In addition, Privacy Act officers in most agencies do not have the stature or the time to monitor compliance with OMB guidelines.

At the present time, there are no general Federal guidelines, statutory or administrative, for the use of front-end verification. The OMB computer matching guidelines specifically exclude from their purview record searches that "verify data in an application for benefits done reasonably soon after the application is received." Front-end verifications done under the Deficit Reduction Act do need to follow the act's requirements for notice, verification, and hearings.

The Data Integrity Boards that S.2756 requires each agency to establish will provide a mechanism through which agencies can oversee computer matching and front-end verification programs. The S.2756 requirement that matching and source agencies submit, to the Data Integrity Boards for approval, written agreements for all matches and front-end verifications will also enhance oversight of these programs. However, it will be important that the Data Integrity Boards follow up to ensure that the terms of the written agreements are being met. If the written agreements merely replace the OMB Checklist, then they will not provide any additional means of agency oversight. It is also important to clarify in the bill whether and how the written agreements would be available to the public so that individuals are provided another channel by which they can receive information on agency practices.

Lack of a Forum to Resolve Conflicts

OTA found that neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved. The efficiency of government programs and investigations is improved by more complete and accurate information about individuals. The societal interest in protecting individual privacy is benefitted by standards and protections for the use of personal information. Public policy needs to recognize and address the tension between these two interests.

Since the Privacy Act was passed in 1974, the primary policy attention with respect to Federal agency administration has shifted away from privacy-related concerns. Interests in management, efficiency, and budget have dominated the executive and legislative agenda in the late 1970s and early 1980s. Congress has authorized information exchanges among agencies in a number of laws, e.g., the Debt Collection Act of 1982 and the Deficit

Reduction Act of 1984. In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

A number of executive bodies have been established to make recommendations for improving the management of the Federal Government, e.g., the President's Council on Integrity and Efficiency, the President's Council on Management Improvement, and the Grace Commission. All have endorsed the increased use of applications such as computer matching, front-end verification, and computer profiling in order to detect fraud, waste, and abuse in government programs. However, these bodies have given little explicit consideration to privacy interests. Some executive guidelines remind agencies to consider privacy interests in implementing new programs, but these are not followed up to ensure agency compliance.

Given the emphasis being placed on Federal management and efficiency, and the sparse oversight of the Privacy Act, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. As a result, decisions about the appropriateness of using certain categories of personal information, such as financial, health, or lifestyle, are often made without the knowledge of or oversight by appropriate agency officials, OMB, Congress, or the affected individuals.

The Data Integrity Boards proposed in S.2756 could provide a forum within each agency in which the tensions between privacy and efficiency could be debated and resolved. The membership of these boards will determine how effective they are in this regard. If the boards are to be balanced, they will need advocates of equal status and expertise representing both interests.

Policy Options

OTA identified a range of policy options for congressional consideration, including those that deal with specific problem areas and others that address institutional changes. If Congress were to do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion, then the present policy problems and confusion will continue. It is likely that the policy emphasis on management efficiency; on detection and prevention of fraud, waste, and abuse; and on effective law enforcement will continue to take precedence over privacy-related concerns. Without congressional action, individuals will continue to be unaware of the majority of uses and disclosures of personal information by Federal agencies because there will be no notice other than that which appears in the Federal Register.

Additionally, absent congressional action, there will be a lack of information available to Congress and the American people -- as well as within agencies themselves -- concerning the scale and scope of information technologies applied to records and record systems in Federal agencies. Therefore, it will continue to be difficult for Congress to exercise effective oversight. Moreover, this lack of information will aggravate the existing difficulties in monitoring the quality, e.g., accuracy and completeness, of personal information that is used and exchanged by Federal agencies.

Addressing Specific Problem Areas -- OTA identified a number of procedural and substantive changes that Congress could legislate. In fashioning such changes, it would be easiest for Congress to address specific problem areas. For example, Congress could establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of information, and the rights of individuals. This is the approach that S.2756 adopts.

In addition, Congress could review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness. More controls and protections for sensitive categories of personal information, such as medical and insurance, could be implemented, as well as controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government. Additionally, Congress could review the use of the social security number as a de facto national identifier and, if necessary, restrict its use or legislate a new universal identification number. Lastly, Congress could review policy with regard to access to the Internal Revenue Service's (IRS) information by Federal and State agencies, as well as with regard to IRS's access to databases maintained by Federal and State agencies and the private sector. If necessary, Congress could legislate a policy that more clearly delineates the circumstances under which such access is permitted.

These changes are not mutually exclusive. Indeed, to provide comprehensive protection for personal information, it may be necessary to legislate in all of these areas. The advantage of this approach is that Congress can specifically tailor solutions to problems. The disadvantage is that it is time-consuming to build separate legislative and political coalitions for each issue. The danger is that some issues may not be debated at all.

Institutional Changes -- OTA found that strengthening an existing institution or establishing a new one would bring more visibility, among the public, Congress, and the agencies, to the issue of personal information collection and use. This could achieve three purposes, either singly or in combination. First, an institution could play the role of an ombudsman in assisting individuals to resolve individual or class grievances with a Federal agency concerning personal information practices. Second, it could oversee Federal agency compliance with the Privacy Act and related OMB guidelines. Third, an institution could provide a forum in which proposals to alter personal information practices and systems could be discussed.

OTA identified four institutional changes available to Congress. The first is to strengthen the role of OMB in the enforcement and oversight of the Privacy Act (for example by requiring OMB to issue regulations and to enforce them) or by enhancing OMB's institutional base for dealing with the Privacy Act (for example by setting up a separate office with responsibility for privacy). Although the institutional framework is in place to achieve these changes quickly, the problem of OMB's commitment to ensuring agency compliance with the Privacy Act remains.

Second, Congress could increase the size, stature, and authority of privacy staff in agencies. The primary problem with this action is that enforcement and oversight responsibilities would be left within the agencies, which may necessitate additional congressional oversight.

Third, Congress could improve its own organization and procedures for consideration of information privacy issues, for example by creating committees with crosscutting privacy jurisdictions, or by providing for better monitoring of bills having information privacy implications and joint referral of such bills to committees with privacy jurisdiction.

Fourth, Congress could establish an entity, such as a Privacy or Data Protection Board, to oversee the personal information practices of Federal agencies. This proposal is not new. In fact, provision for a permanent Privacy Protection Commission was included in the original Privacy Act that passed the Senate. In 1977, the Privacy Protection Study Commission recommended the establishment of a Federal Privacy Board. Most Western European countries and Canada have established boards or commissions with responsibilities for the protection of personal information. The advantages and disadvantages of a new privacy authority in the United States would be determined by the design of the agency and the powers with which it is vested.

S.2756 requires that each agency establish a Data Integrity Board. This is an important institutional change at the agency level and will provide a mechanism for congressional oversight of agency activities in this area. However, S.2756 does not provide a direct means for arriving at the comprehensive picture of Federal activities in this area. OTA found that such an overall picture is important to realizing the scale and scope of Federal personal information exchanges and uses. Although it could be compiled by reviewing the files of each Data Integrity Board, this may not occur. Therefore, the larger issues, such as the creation of a *de facto* national database and use of the social security number as a *de facto* national identifier, may not be addressed.

Summary

S.2756, the Computer Matching and Privacy Protection Act of 1986, addresses many of the problems that OTA identified with regard to computer matching and front-end verification. The written agreements that a matching agency and a source agency are to develop prior to a match, and the approval of these agreements by the Data Integrity Boards, should ensure that matches are not done at the discretion of program managers and should enable agencies to improve their oversight of the match and its results.

The provisions of S.2756 for notice of matching programs will make statutory the existing OMB requirement that matches be reported in the *Federal*

Register. Moreover, S.2756 restores the requirements for a 30-day public comment period and for advance notice to Congress and OMB, which were contained in the 1979 OMB Guidelines and eliminated in the 1982 Guidelines. S.2756 also extends these requirements to front-end verification programs.

Additionally, S.2756 requires agencies to specify in the written agreements the procedures for providing notice to individuals whose records are being used in a matching or front-end verification program. The implication is that this notice would be in addition to the notice in the Federal Register; however, it is possible that an agency would specify its notice procedure as being the Federal Register notice. The OTA findings indicate that some notice that is more directly addressed to individuals is necessary to conform to the goals of the Privacy Act.

The provision for agency Data Integrity Boards may be the most important section of the bill, as it provides for an institutional enforcement mechanism. The boards are given several functions, including: approving all matching agreements; reviewing all recurring matching programs; and serving as the principal policymaker and overseer of the agency's implementation of the Computer Matching and Privacy Protection Act. The boards, however, have no role in assisting individuals in finding out about the uses of personal information or in bringing questions, complaints, or grievances to an agency. In order for this board to be most effective, it will be necessary that a balance between the interests of management efficiency and privacy be equally maintained. If this board were to be dominated by one interest or the other, it would not serve well the interests that S.2756 seeks to protect.

The requirement for independent verification of information before it can be used in an adverse action against an individual addresses the existing problems of data quality and is an important step in minimizing the use of inaccurate or incomplete personal information. Statutory provisions for an individual's opportunity to refute information, to be notified of an adverse decision before any action is taken, and to have a hearing are also important in clarifying individual rights and remedies.

In conclusion, S.2756 addresses many of the problems identified in the OTA report. S.2756 is a significant first step toward exercising statutory control over Federal agency use of computer matching and front-end verification.

II

99TH CONGRESS
2D SESSION

S. 2756

To amend title 5 of the United States Code, to ensure privacy, integrity, and verification of data disclosed for computer matching, to establish Data Integrity Boards within Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

AUGUST 14 (legislative day, AUGUST 11), 1986

Mr. COHEN (for himself and Mr. LEVIN) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

---

A BILL

To amend title 5 of the United States Code, to ensure privacy, integrity, and verification of data disclosed for computer matching, to establish Data Integrity Boards within Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Matching and Privacy Protection Act of 1986".

SEC. 2. MATCHING AGREEMENTS.

(a) IN GENERAL.—Subsection (b) of section 552a of title 5, United States Code, is amended—

(1) by striking out "or" at the end of paragraph (11),

(2) by striking out the period at the end of paragraph (12) and inserting in lieu thereof "; or", and

(3) by adding at the end thereof the following new paragraph:

"(13) to a matching agency or a non-Federal matching entity pursuant to a written matching agreement under subsection (o) of this section.".

(b) MATCHING AGREEMENTS.—Section 552a of title 5, United States Code, is amended—

(1) by redesignating subsections (o), (p), and (q) as subsections (p), (q), and (r), respectively, and

(2) by inserting after subsection (n) the following new subsection:

"(o) MATCHING AGREEMENTS.—At least 30 days prior to disclosing any record to a matching agency or non-Federal matching entity for use in a computer matching program or front-end eligibility verification program, a source agency and the matching agency or non-Federal matching entity shall enter into a written agreement specifying—

"(1) the justification, purpose, and legal authority for conducting the program;

"(2) a description of the records that will be matched, including the data elements that will be used, the number of records that will be matched, and the projected starting and completion dates of the matching program;

"(3) that individuals whose records are matched will be notified of such matching program or front-end eligibility verification program and the procedures for providing such notice;

"(4) that information produced by matching programs or front-end eligibility verification programs will be verified and the method of such verification;

"(5) that records created by such program shall be retained only so long as an investigation, either criminal or administrative, is active, and procedures for destroying such records created by the program;

"(6) safeguards to ensure administrative, technical, and physical security of the records matched and the results of such programs;

"(7) prohibitions on the duplication or redisclosure of records provided by the source agency within or outside the matching agency or non-Federal matching entity conducting the matching program or front-end eligibility verification program, unless authorized by the source agency;

"(8) prohibitions on the extraction or compilation of data on individuals who are not identified as a result of the matching program or front-end eligibility verification program;

"(9) terms and conditions governing the use of the records provided by the source agency for use in a matching program or front-end eligibility verification program, such as procedures governing return to source agency or destruction of records used in such program; and

"(10) information on any reliability assessments that have been conducted on the records that will be matched.".

SEC. 3. NOTICE OF MATCHING PROGRAMS OR FRONT-END ELIGIBILITY VERIFICATION PROGRAMS.

(a) NOTICE IN FEDERAL REGISTER.—Subsection (e) of section 552a of title 5, United States Code, is amended—

(1) by striking out "and" at the end of paragraph (10),

(2) by striking out the period at the end of paragraph (11) and inserting in lieu thereof "; and", and

(3) by adding at the end thereof the following new paragraph:

"(12) with respect to any establishment or revision of a matching program or front-end eligibility verification program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.".

(b) REPORT TO CONGRESS AND OFFICE OF MANAGEMENT AND BUDGET.—

(1) IN GENERAL.—Subsection (p) of section 552a of title 5, United States Code, as redesignated by section 2(b)(1) of this Act, is amended by striking out "system of records" and inserting in lieu thereof "system of records, matching program, or front-end eligibility verification program".

(2) CLERICAL AMENDMENT.—The heading of such subsection (p) is amended by inserting "OR PROGRAMS" after "SYSTEMS".

SEC. 4 DATA INTEGRITY BOARD.

Section 552a of title 5, United States Code, as amended by section 2(b)(1) of this Act, is amended by adding at the end thereof the following new subsection:

"(s)(1) DATA INTEGRITY BOARDS.—Every agency shall establish a Data Integrity Board to oversee and coordinate the agency's implementation of this section.

"(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, including the senior official responsible for agency administration, the senior official designated under section 3506(b) of title 44, United States Code, and any senior official designated by the head of the agency as responsible for implementation of this section.

"(3) Each Data Integrity Board shall perform the following functions:

"(A) serve as the principal policymaker and overseer of the agency's implementation of this section;

"(B) develop, review, and coordinate privacy training programs for the agency's personnel;

"(C) review, approve, and maintain all written agreements for disclosure of agency records for matching programs or front-end eligibility verification programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

"(D) annually review all matching programs and front-end eligibility verification programs in which the agency has participated during the year, either as a source agency or matching agency, to determine compliance with applicable laws, regulations, and agency agreements;

"(E) annually review all recurring matching programs in which the agency has participated during the year, either as a source agency or matching agency, continued justification for such disclosures, and compliance with applicable laws, regulations, and agency agreements;

"(F) compile an annual report to the head of the agency, the Office of Management and Budget, and the Congress on the matches in which the agency has participated as a source agency or matching agency;

"(G) receive information on the accuracy and reliability of records provided by the source agency for use in matching programs or front-end eligibility verification programs;

"(H) provide interpretation and guidance to agency components and personnel on the requirements of this section; and

"(I) review agency recordkeeping and disposal policies and practices to assure compliance with this section.

"(4) Each Data Integrity Board shall maintain such staff as necessary to carry out its functions specified by this subsection. Such staff shall include persons designated by the head of the agency as responsible for implementation of this section.".

SEC. 5. VERIFICATION.

(a) In General.—Notwithstanding any other provision of law, in order to protect any individual whose records are used in matching programs or front-end eligibility verification programs, no matching agency or non-Federal matching entity may deny, terminate, suspend, or reduce any Federal financial assistance to such individual, or take other adverse action against such individual as a result of information produced by such programs, until such agency or entity has independently verified such information. Such independent verification may be from third-party sources or the individual whose records are matched.

(b) INDEPENDENT VERIFICATION.—Independent verification required by subsection (a) of this section shall relate to—

(1) the amount of the asset or income involved,

(2) whether such individual actually has or had access to such asset or income for such individual's own use, and

(3) the period or periods when the individual actually had such asset or income.

(c) OPPORTUNITY TO REFUTE INFORMATION.—Notwithstanding any other provision of law, no matching agency or non-Federal matching entity may deny, terminate, suspend, or reduce any Federal financial assistance to any individual described in subsection (a), or take other adverse action against such individual as a result of information produced by a matching program or a front-end eligibility verification program, until such agency or entity has provided such individual an opportunity to refute the information produced by such program.

(d) NOTICE OF DECISION.—Notwithstanding any other provision of law, in all cases involving denial, reduction, suspension, or termination of Federal financial assistance as a result of information produced by a computer matching program or front-end eligibility verification program, an individual shall be provided with notice of the findings of the matching agency or non-Federal matching entity made on the basis of verified information, of the adverse action to be taken, and information on the right to appear and any opportunity for a hearing.

(e) SANCTIONS.—Notwithstanding any other provision of law, no source agency may disclose any record or system of records to a matching agency or non-Federal matching entity for a matching program or front-end eligibility verification program if such source agency has reason to believe that the requirements of this section and any matching agreement entered into pursuant to section 552a(o) of title 5, United States Code, are not being met by such matching agency or entity.

(f) DEFINITIONS.—For purposes of this section—

(1) The terms "matching program", "front-end eligibility verification program", "matching agency", "non-Federal matching entity", "record", and "source agency" shall have the meanings given to such terms by section 552a(a) of title 5, United States Code.

(2) The term "Federal financial assistance" means any assistance provided through a Federal grant, loan, or contract of insurance or guaranty.

SEC. 6. DEFINITIONS.

Subsection (a) of section 552a of title 5, United States Code, is amended—

(1) by striking out "and" at the end of paragraph (6),

(2) by striking out the period at the end of paragraph (7) and inserting in lieu thereof a semicolon, and

(3) by adding at the end thereof the following new paragraphs:

"(8) the term 'matching program' means any computerized comparison of two or more automated systems of records or a system of records with a set of non-Federal records to identify individuals common to two or more of the systems of record or unique to one of the systems of record, but such term does not include—

"(A) matches done to produce a statistical record; or

"(B) matches performed by an agency in which no records or systems of records are disclosed to other agencies or non-Federal entities;

"(9) the term 'front-end eligibility verification program' means the certification of accuracy of information supplied by an applicant for Federal financial assistance (as defined in section 5(e)(2) of the Computer Matching and Privacy Protection Act of 1986) by matching such information against a computerized data base;

"(10) the term 'matching agency' means any agency performing a matching program;

"(11) the term 'source agency' means the agency which discloses records from a system of records to be used in a matching program or a front-end eligibility verification program; and

"(12) the term 'non-Federal matching entity' means any State or local government, or agency thereof, which acts as a matching or source agency for matching programs or front-end eligibility verification programs involving Federal Government data.".

Federal Fegister, May 19, 1982, 47 FR 21656

OFFICE OF MANAGEMENT AND BUDGET

Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs

May 14, 1982.

AGENCY: Office of Management and Budget.

ACTION: Issuance of Revised Guidance for Conducting Computerized Matching Programs

SUMMARY: This document revises and updates guidance to the agencies on conducting automated matching programs originally issued on March 30, 1979.

EFFECTIVE DATE: May 11, 1982.

FOR FURTHER INFORMATION CONTACT: Robert N. Veeder, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 3235, New Executive Office Building, Washington, D.C. 20502; telephone (202) 395-4814.

SUPPLEMENTARY INFORMATION: The Guidelines were originally issued on March 30, 1979 (44 FR 23138). After evaluating agencies experiences operating under those Guidelines and considering comments from agencies and concerned groups such as the President's Council on Integrity and Efficiency in Government, OMB concluded that a revision was in order. Accordingly, the Guidelines were revised to clarify the language and to simplify, where possible, the administrative and procedural requirements.

The Revised Guidelines were signed by the Director of OMB on May 11, 1982, and became effective on that date. Their text is set forth below.

Brenda A. Mayberry,

Acting Budget and Management Officer.

May 11, 1982.

Memorandum for the Executive Departments and Establishments

From: David A. Stockman, Director.

Subject: Revised Supplemental Guidance for Conducting Matching Programs.

I am attaching a copy of our revised Guidelines on conducting computerized matching programs. This revision updates and simplifies earlier guidance issued on March 30, 1979. It is effective immediately.

The revision is the result of our evaluation of agencies' operating experiences under the original Guidelines. The new Guidelines incorporate many agency recommendations for clarifications and changes. In addition, they greatly simplify the notice and reporting requirements of the earlier version.

Direct comments or questions on these Guidelines to OMB's Office of Information and Regulatory Affairs.

Matching Guidelines

1. *Purpose*—These Guidelines supplement and should be used in conjunction with the "OMB Guidelines on the Administration of the Privacy Act of 1974," issued on July 1, 1975 and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concerns expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." These Guidelines do not authorize activities which are not permitted by law; nor do they prohibit activities expressly required to be performed by law. Complying with these Guidelines, however, does not relieve a Federal agency of the obligation to comply with the provisions of the Privacy Act, including any provisions not cited in these Guidelines.

2. *Scope*—These guidelines apply to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a), and to all matching programs:

a. Performed by a Federal agency, whether the personal records used in the match are Federal or non-Federal.

b. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any non-Federal organization.

3. *Effective Date*—These guidelines are effective on their date of issuance—May 11, 1982.

4. *Definitions*—For the purposes of these Guidelines:

a. All the terms defined in the Privacy Act of 1974 apply.

b. A "personal record" means any information pertaining to an individual that is stored in an automated system of records, e.g., a data base which contains information about individuals that is retrieved by name or some other personal identifier.

c. A "matching program" is a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among a number of participants.

Matching Programs do not include the following:

(1) Matches which do not compare a substantial number of records, e.g., comparison of the Department of Education's Defaulted Student Loan data base with the Office of Personnel Management's Federal Employee data base would be covered; comparison of six individual student loan defaultees with the OPM file would not be covered.

(2) Checks on specific individuals to verify data in an application for benefits done reasonably soon after the application is received.

(3) Checks on specific individuals based on information which raises questions about an individual's eligibility for benefits or payments done reasonably soon after the information is received.

(4) Matches done to produce aggregate statistical data without any personal identifiers.

(5) Matches done to support any research or statistical project where the specific data are not to be used to make decisions about the rights, benefits, or privileges of specific individuals.

(6) Matches done by an agency using its own records.

d. A "matching agency" is the Federal agency which actually performs the match.

e. A "source agency" is the Federal agency which discloses records from a system of records to be used in the match. Note that in some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match. The disclosure of records to the matching agency and any subsequent disclosure of "hits" (by either the matching or the source agencies) must be done in accordance with the provisions of paragraph (b) of the Privacy Act.

f. A "hit" is the identification, through a matching program, of a specific individual.

5. *Guidelines for Agencies Participating in Matching Programs*—Agencies should acquire and disclose matching records and conduct matching programs in accordance with the provisions of this section and the Privacy Act.

a. Disclosing Personal Records for Matching Programs

(1) To Another Federal Agency—source agencies are responsible for

determining whether or not to disclose personal records from their systems and for making sure they meet the necessary Privacy Act disclosure provisions when they do. Among the factors source agencies should consider are:

(a) Legal authority for the match;

(b) Purpose and description of the match;

(c) Description of the records to be matched;

(d) Whether the record subjects have consented to the match; or whether disclosure of records for the match would be compatible with the purpose for which the records were originally collected, i.e., whether disclosure under a "routine use" would be appropriate; whether the soliciting agency is seeking the records for a legitimate law enforcement activity—whichever is appropriate; or any other provision of the Privacy Act under which disclosure may be made;

(e) Description of additional information which may be subsequently disclosed in relation to "hits";

(f) Subsequent actions expected of the source (e.g., verification of the identity of the "hits" or follow-up with individuals who are "hits").

(g) Safeguards to be afforded the records involved, including disposition.

If the agency is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, it may proceed to make the disclosure to the matching agency. It should ensure that only the minimum information necessary to conduct the match is provided. If disclosure is to be made pursuant to a "routine use" (Section (b)(3) of the Privacy Act), it should ensure that the system of records contains such a use, or it should publish a routine use notice in the Federal Register. The agency should also be sure to maintain an accounting of the disclosures pursuant to section (c) of the Privacy Act.

(2) To a Non-Federal Entity—Prior to disclosing records to a non-Federal entity for a matching program to be carried out by that entity, a source agency should, in addition to all of the considerations in 5a(1) above, also make reasonable efforts, pursuant to section (e)(6) of the Privacy Act, to "assure that such records are accurate, complete, timely, and relevant for agency purposes."

b. Written Agreements—Prior to disclosing to either a Federal or non-Federal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file, e.g.: That the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file(s) previously agreed to; that it will not be used to extract information concerning "non-hit" individuals for any purpose; and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency.

c. Performing Matching Programs—

(1) Matching agencies should maintain reasonable administrative, technical and physical security safeguards on all files involved in the matching program.

(2) Matching agencies should insure that they have appropriate systems of records including those containing "hits," and that such systems and any routine uses have been appropriately noticed in the **Federal Register** and reported to OMB and the Congress as appropriate.

d. Disposition of Records—

(1) Matching agencies will return or destroy source matching files (by mutual agreement) immediately after the match.

(2) Records relating to hits will be kept only so long as an investigation, either criminal or administrative, is active and will be disposed of in accordance with the requirements of the Privacy Act and the Federal Records Schedule.

e. Publication Requirements—

(1) Agencies, prior to disclosing records outside the agency, will publish appropriate "routine use" notices in the **Federal Register**, if necessary.

(2) If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, the agency involved should publish the appropriate **Federal Register** notice and submit the requisite report to OMB and the Congress pursuant to OMB Circular No. A-108.

f. Reporting Requirements—

(1) As close to the initiation of the matching program as possible, matching agencies shall publish in the **Federal Register** a brief public notice describing the matching program. The notice should include:

(a) The legal authority under which the match is being conducted;

(b) A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose(s) for which the program is being conducted, and the procedures to be used in matching and following up on the "hits";

(c) A complete description of the personal records to be matched, including the source(s), system of records identifying data, date(s) and page number(s) of the most recent **Federal Register** full text publication where appropriate;

(d) The projected start and ending dates of the program;

(e) The security safeguards to be used to protect against unauthorized access or disclosure of the personal records; and

(f) Plans for disposition of the source records and "hits."

Agencies should send a copy of this notice to the Congress and to the Office of Management and Budget at the same time it is sent to the Federal Register.

(2) Agencies should report new or altered systems of records as described in e (2) above as necessary.

(3) Agencies should also be prepared to report on matching programs pursuant to the reporting requirements of either the Privacy Act or the Paperwork Reduction Act. Reports will be solicited by the Office of Information and Regulatory Affairs and will focus on both the protection of individual privacy and the government's effective use of information technology. Reporting instructions will be disseminated to the agencies as part of either the reports required by section (p) of the Privacy Act or section 3514 of Pub. L. 96-511.

g. Use of Contractors—Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contract. When contractors are used, however,

(1) The matching agency should, consistent with subsection (m) of the Privacy Act, cause the requirements of that Act to be applied to the contractor's performance of the matching program. The contract should include the Privacy Act clause required by FPR Amdt. 155, 41 CFR 1-1.337-5;

(2) The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards and guidelines issued by OMB, GSA, and the Department of Commerce;

(3) The terms of the contrct should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;

(4) Contractor personnel involved in the matching program should be made explicitly aware of their obligations under the Act, and of these guidelines, agency rules and any special safeguards in relation to each specific match performed.

(5) Any disclosures of records by the agency to the contractor should be made pursuant to a "routine use" (Section (b)(3) of 5 U.S.C. 552a).

6. *Implementation and oversight*— the Office of Management and Budget will oversee the implementation of these Guidelines and shall interpret and advise upon agency proposals and actions within their scope, consistent with section 6 of the Privacy Act.

[FR Doc. 82-13883 Filed 5-19-82; 8:45 am]

BILLING CODE 3110-01-M

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 29, 1983

M-84-6

MEMORANDUM TO: HEADS OF EXECUTIVE DEPARTMENTS, ESTABLISHMENTS, AND INDEPENDENT AGENCIES

FROM: Joseph R. Wright, Jr.
Deputy Director

SUBJECT: Computer Match Checklist and Model Control System and Resource Document for Conducting Computer Matching Projects Involving Individual Privacy Data

The purpose of this memorandum is to provide instructions for the preparation of a Computer Match Checklist to be completed by each department and agency engaging in or providing data for computer matching of Federal data records conducted by Federal, State or local entities. This Checklist and the "Model Control System and Resource Document for Conducting Computer Matching Projects Involving Individual Privacy Data" transmitted by this memorandum are intended to assist agencies in complying with the requirements of the Privacy Act of 1974 and the OMB Computer Matching Guidelines issued May 11, 1982.

The Computer Match Checklist must be completed for each agency computer match and maintained on file within the agency for review by OMB, GAO or other Federal entities. The Model Control System is intended to provide guidance to agencies in developing and maintaining adequate internal agency controls over the approval and conduct of computer matching activities.

The Computer Match Checklist is a requirement and applies to all agencies subject to the Privacy Act of 1974 (5 U.S.C. 552a), and to all matching programs:

a. Performed by a Federal agency, whether the personal records used in the match are Federal or non-Federal.

b. For which a Federal agency discloses any personal records for use in a matching program performed by any other Federal agency or any non-Federal organization.

The Model Control System is the recommended approach for agencies to follow in approving and overseeing proposed computer matching activities. The model procedure outlined is recommended, not required. However, there should be a suitable rationale whenever an agency does not follow the model approach.

For the purpose of this memorandum:

a. All the terms defined in the Privacy Act of 1974 apply.

b. All the terms defined in the OMB Computer Matching Guidelines issued May 11, 1982 apply.

The Computer Match Checklist is to be completed by both the source and sponsoring department or agency immediately following publication of an intent to match in the Federal Register. The Checklist is to be maintained on file and will be used by the agency or department in completing their submission to the Office of Management and Budget under the reporting requirements of the Privacy Act of 1974. This file will also be available for review by OMB, GAO and other Federal entities to insure proper safeguards are being used to protect personal data and to oversee agency management computer match decision-making.

Inquires concerning this memorandum or the Model Control System for Computer Matching should be directed to the Office of Management and Budget, Interagency Activities Division, 395-3692.

Attachments

Attachment A

Agency Computer Match Checklist

This Checklist shall be completed for each department or agency computer match (including those in which the department or agency is the source of personal data for a non-Federal match) immediately following publication of the matching report in the *Federal Register* (or release of data for a non-Federal match). This Checklist is be maintained on file for review by OMB, GAO and other Federal entities.

a. Has the agency sent a new/altered Privacy Act System Report to OMB and Congress? (check one)

Yes _____. Date sent: ______________________________

No _____. A report is not required. Why? ________
____
____

b. Has the agency published in the *Federal Register* a new/altered system notice?

Yes _____. Published on: ______________________________

No _____. A notice is not required. Why? ____________
____
____

c. Have all participating sources and matching agencies published routine use notices in the *Federal Register*?

Yes _____.

Agencies:	Date of Routine Use Notice Publication:
____________________	____________________
____________________	____________________
____________________	____________________

No _____, (attach explanation).

d. Have written agreements between the Federal source agencies and Federal or non-Federal matching agencies been exchanged listing conditions for the match and safeguards for individual records (OMB Matching Guidelines - Section 5b)?

Yes _____.

No _____. Reason and date when agreements will be exchanged: ______________________________

e. When was the Agency Computer Match Report published in the Federal Register (not applicable if a Federal agency is only a source for the match).

Date of Federal Register publication: ________________

Date sent to OMB and Congress: ______________________
(attach Federal Register notice)

f. What is the estimated number of individuals whose records are to be matched (by the following categories)?

o benefit records: ______________________________

o personnel/employment records: ______________________

o indebtedness/accounts receivable records: ____________

o provider records: ______________________________

o other (describe):______________________________

g. If contractors are being used, have proper controls been instituted as outlined in Section 5g, of OMB's Computer Matching Guidelines, issued May 11, 1982?

Yes ____________. Date of Agreement: ________________
(attach copy of contract clause).

No ____________. (include an estimate when contract or revisions will be signed and assurances that contractors will not participate until that time.)

h. When will cost/benefit analysis on the computer match be available?

Date: ____

Estimated cost/benefit figures are required to be attached to this form and be made available to OMB upon request.

____
Signature of Completing Official

MODEL CONTROL SYSTEM AND RESOURCE DOCUMENT FOR CONDUCTING COMPUTER MATCHING PROJECTS INVOLVING INDIVIDUAL PRIVACY DATA

Office of Management and Budget
President's Council on Integrity and Efficiency

TABLE OF CONTENTS

Page

I. Introduction. 1
II. Definition. 2
III. Background. 2
IV. The Model Control System. 4

Attachments:

A. Model System Flow Chart and Document/ Process Narratives. 5

B. Systems of Records Notices. 19
B1 VA System Notice
B2 OPM System Notice

C. HHS Notice of Intent to Establish a System of Records. 31

D. Source Agency Data File Format and Specifications. 37

E. Source Agency Routine Use Notices 45
E1 HHS Routine Use Notice
E2 OPM Routine Use Notice

F. Matching Agency (VA) Routine Use Notice 55
F1 Request for Publication of Notice
F2 Notice as Published in the Federal Register

G. VA Matching Report Submissions. 63
G1 Submission for Federal Register Publication
G2 Submission to OMB and Congress

H. Matching Reports in the Federal Register. . . .81
H1 HHS-Office of Inspector General
H2 HHS-Social Security Administration
H3 VA-Office of Inspector General

Model Control System and Resource Document
for
Conducting Computer Matching Projects
Involving Individual Privacy Data

I. Introduction

Computer matching is being used by most Inspectors General and program managers to identify fraud, waste and abuse. Regarded as an effective management tool, matching techniques can be used to examine extremely large amounts of computerized data quickly and efficiently.

Two of the most important ingredients of most computer matching projects are protecting the privacy of individuals and complying with the legal/policy requirements of the "Revised Supplemental Guidance for Conducting Matching Programs" (OMB Memorandum M-82-5) dated May 11, 1982, hereinafter referred to as the OMB Matching Guidelines. Generally, these guidelines apply to all match projects using automated files which contain individual privacy data. Compliance with the OMB Matching Guidelines is critical for the protection of personal privacy and the avoidance of unwarranted harassment of individuals.

This document provides an approach to conducting computer matching projects which meets the requirements of the OMB Matching Guidelines. Specifically, it:

- Provides background and definitive information pertaining to computer matching.
- Provides a methodology for assuring that adequate protection is afforded privacy data used during computer matching.
- Presents a model control system, i.e., a set of processes and procedures for successfully undertaking computer matching programs involving individual privacy data.

The model control system is intended to assist in the preparation for and conduct of computer matching programs involving personal-data files from any element of the Executive Branch of the Federal Government. Though each and every individual document or process step may not be applicable for a particular matching program, use of the model should assure compliance with privacy and procedural requirements of the Privacy Act and the OMB Matching Guidelines and thus help to ensure a successful matching program.

II. Definitions

For the purposes of this document:

- A computer match is the computerized comparison of two or more automated systems of records, at least one of which is a Federal system, to identify individuals common to two or more of the record systems or unique to one of the record systems.
- All the terms defined in the Privacy Act of 1974 apply.
- All the terms defined in the OMB Matching Guidelines apply.

III. Background

In the Privacy Act of 1974, Congress expressed concern that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information." The Act, therefore, makes any system of records from which information is retrieved using personal identifiers (such as name, SSN, or claim number) subject to its provisions and, by derivation, to those of any supplemental or implementing guidelines and instructions pertaining to the Act. For computer matching, the significant supplemental or implementing documents are (1) OMB Matching Guidelines; (2) OMB Circular No. A-108, July 1, 1975, as amended; and (3) OMB Guidelines on the Relationship Between the Privacy Act of 1974 and the Debt Collection Act of 1982.

The Privacy Act of 1974

The Privacy Act provides specific guidance concerning privacy protection of personal data and identifies actions required of agencies maintaining such data.

The Privacy Act also establishes the right of each individual to have some control over the information which the Federal government maintains about him or her in a personally identifiable and retrievable format. Within limitations defined by law, an individual can: determine what records are collected, maintained, used, or disseminated; prevent disclosure of information for any purposes other than the ones for which collected; gain access to the information maintained; and sue for damages which occur as a result of willful or intentional agency action which violates his or her rights under the Act.

OMB Matching Guidelines

The OMB Matching Guidelines provide guidance for Federal agencies participating in computer matching programs. Procedures and reporting requirements are given for both the agency performing the match (matching agency) and the agency(ies) disclosing records to the matching agency for use in the match (source agency(ies)).

Paragraph 4.c. of the OMB Matching Guidelines defines the term "matching program" and describes six types of matches which are not matching programs as defined. Those six types are not subject to the guidelines. Any computer match or related series of matches meeting the definition of a matching program must be conducted in accordance with the OMB Matching Guidelines.

OMB Circular No. A-108, as amended.

OMB Circular No. A-108 provides guidance to Federal agencies for implementing the Privacy Act. Like the Privacy Act, Circular A-108 is applicable to the creation and maintenance of systems of records containing individually-identifiable, personal information.

Of particular importance for computer matching is Transmittal Memorandum (TM) No. 1 to Circular A-108, September 30, 1975, as amended by TM No. 3, May 17, 1976. TM No. 1 contains instructions for preparing the "Report of Intention to Establish or Alter Systems of Personnel Records." This report must be prepared whenever the results of a computer matching program create or significantly alter a system of records subject to the Privacy Act. In addition, a System of Records Notice must be printed in the Federal Register. Samples of system notices are at Attachment B. A sample notice of intent to establish a new system of records is at Attachment C.

OMB Guidelines on the Relationship Between the Privacy Act of 1974 and the Debt Collection Act of 1982

These OMB guidelines address in detail the following changes and conditions created by the Debt Collection Act. The Debt Collection Act:

- Amends the Privacy Act of 1974 to provide a new general disclosure authority, subsection (b)(12), which lets agencies disclose personal information to consumer reporting agencies.

- Creates a statutory authority to satisfy the conditions established by the Privacy Act whereby agencies can make disclosures under subsection (b)(3) "for a routine use." The Privacy Act requires that such disclosures be compatible with the purpose for which the information was originally collected. The routine use disclosures which the Debt Collection Act authorizes include disclosures of taxpayer mailing addresses in certain instances, as well as disclosures of debtor information to effect administrative or salary offsets.

- Creates statutory authority for agencies to collect the Social Security Account Number from applicants in certain Federal loan programs.

- Amends the Privacy Act to exempt consumer reporting agencies from the "contractor" provisions of the Privacy Act.

IV. The Model Control System

The objective of the model control system is to provide a procedural guide for conducting computer matching projects while complying with the Privacy Act and the OMB Matching Guidelines. Agencies do not have to adopt the model per se, but should use it as guidance. The main purpose of the model is to achieve a successful project conclusion with due regard for personal privacy and individual rights.

The model control system is presented in flow chart form with narrative statements keyed to critical action points at various stages in the project. The narrative statements provide suggested approaches for accomplishing a computer matching project. References to specific OMB Matching Guidelines requirements are indicated for each document/process step.

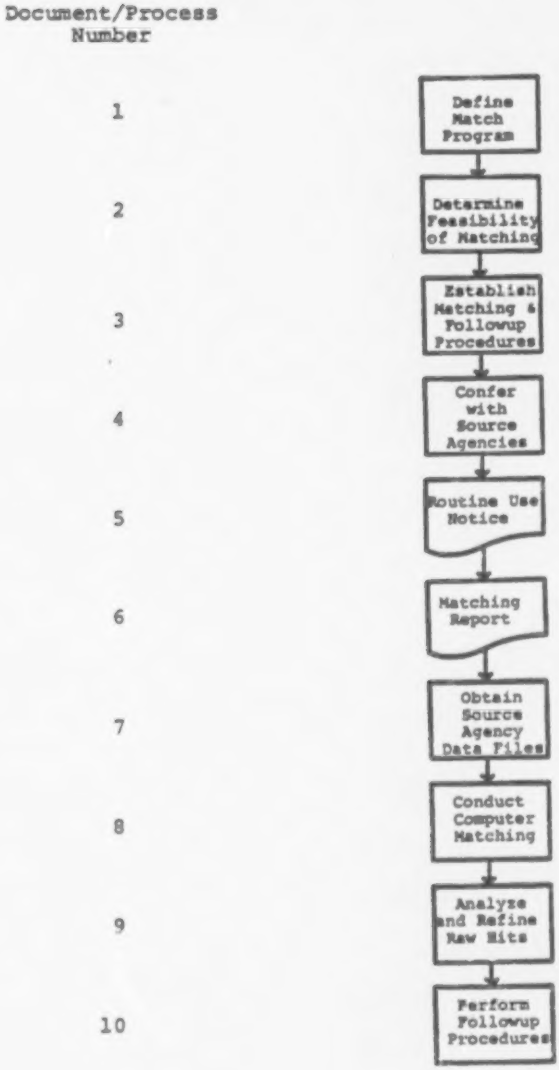
The Model Control System Flow Chart and the narratives for the ten document/process steps are at Attachment A.

Attachment A

Model System Flow Chart and Document Process Naratives

Attachment A

Model Control System
for
Conducting Computer Matching Projects Involving Individual Privacy Data


Document/Process Number
1
Define Match Program
2
Determine Feasibility of Matching
3
Establish Matching & Followup Procedures
4
Confer with Source Agencies
5
Routine Use Notice
6
Matching Report
7
Obtain Source Agency Data Files
8
Conduct Computer Matching
9
Analyze and Refine Raw Hits
10
Perform Followup Procedures

Document/Process No. 1

Define
Match
Program

Description: A determination must be made as to whether your project is associated with automated records and is susceptible to computer matching techniques. If you determine that your task can be expedited or your scope expanded through the use of matching techniques, then you must determine the applicability of the OMB Matching Guidelines and ensure compliance therewith.

OMB Matching Guidelines Reference: Paragraph 4.c.

Suggested Approach:

- Determine the goals or desired results of the match.
- Identify the information or source data required and determine if these data are automated.
- Identify sources of the automated data; e.g., Federal agencies, nongovernmental agencies.
- Determine whether these automated files contain privacy data and are protected by the Privacy Act and the provisions of OMB Circular A-108.
- Determine whether the match program is subject to the OMB Matching Guidelines.

Document/Process No. 2

Determine
Feasibility
of Matching

Description: Once you have determined that your project involves matching of automated records, you should identify various alternatives of accomplishment. The most effective method of accomplishing your objectives should be your primary goal, giving full consideration to a comparison of costs versus benefits for each alternative.

OMB Matching Guidelines Reference: Paragraph 4.f.

Suggested Approach:

- Determine the feasibility of a manual comparison of records.
- Determine if desired information is available from some source agency in a usable format which could eliminate the need for a matching program.
- Identify the estimated costs of the matching program, including verification of hits.
- Estimate the benefits of the match results.
- Establish the feasibility of an automated approach.
- Select the most appropriate method.

Document/Process No. 3

Establish
Matching &
Followup
Procedures

Description: This process develops the foundation on which the match project rests. The procedures established, subject to refinement as the project progresses, will govern the actions necessary for data collection, computer processing, analysis of hits, and followup actions, including recoupment and civil and criminal litigation. The procedures provide a major portion of the content of the matching report.

OMB Matching Guidelines Reference: Paragraph 5.

Suggested Approach:

- Establish and refine match criteria which will reduce errors in the project and provide greater integrity to your match results.
- Determine what information will be needed from the source agency or agencies.
- Define the processes for data collection to include file formats, data content, data sources, and methods of acquisition.
- Establish data handling procedures to include all privacy and computer security considerations for transporting, storing, processing, and disposing of data files whether acquired from source agencies or created during the match.
- Establish procedures for analysis, validation, and purification of hits to preclude harassment and invasion of the privacy of individuals identified as raw hits but not found to be valid hits.
- Design followup actions which will terminate benefits and/or initiate collection and recoupment giving full regard to protection of the innocent. The Debt Collection Act of 1982 should be considered during this step.
- Design a process for collecting matching program costs and results and developing cost/benefit information for use in after-action reports and in planning for subsequent matches.

Document/Process No. 4

Confer
with
Source
Agencies

Description: This step permits the matching agency to present its matching and followup plans to the source agencies and obtain a consensus about how the various parties will interact during the project. The need for routine use notice publication by Federal source agencies should be discussed. Other actions which the source agencies must perform to provide the source data files should be defined and agreement reached for them to be initiated.

OMB Matching Guidelines Reference: Paragraphs 4.d., 4.e., 5.a., 5.b., 5.e.

Suggested Approach:

- Present the ground rules for the project to all source agencies. The "ground rules" are the procedures established in Process No. 3.
- Obtain general agreement with the ground rules from each source agency. Where disagreements arise, attempt to modify the procedures, if possible, so that agreement can be reached.
- Establish the types of coordination and cooperation which will be required as the project progresses.
- Discuss privacy restrictions on data needed for the match. If dealing with a Federal agency, determine if an existing routine use permits disclosure of required data.
- If a new routine use is required for a Federal source agency data file, identify the routine use needs and obtain agreement from the source agency's system manager to initiate publication actions.
- Provide each source agency with the format and specifications which you wish to be used for preparation of the source agency data files. A sample record format and file specification is at Attachment D.
- Establish the processes by which each source agency will obtain the written agreements outlined in paragraph 5.b. of the OMB Matching Guidelines.

Document/Process No. 5

Routine Use Notice

Description: If existing Federal privacy system notices do not include a routine use which permits disclosure, new routine uses should be established. The routine use notices required for each participating agency are developed and released for publication in the Federal Register. A minimum of 60 days should be allowed from start of this procedure through the 30-day waiting period after initial publication. If any significant challenges to a notice are received, 30 or more additional days may be required before data can be released to or by the matching agency.

OMB Matching Guidelines Reference: Paragraphs 5.a.(1)(d), 5.b., 5.c., 5.e.

Suggested Approach:

- Submit a formal, written request to each source agency for publication of routine use notices. In this letter, the matching agency should provide all information which the source agencies require to prepare the routine use notices. Sample source-agency routine use notices are at Attachment E.
- Publish routine use notices governing release of data generated by the match. A request from the official in charge of the match to the department responsible for the files to be matched might be required. A sample of such a request, which could also be a guide for letters to the source agencies, along with a sample matching-agency routine use notice are at Attachment F.

If the matching program will create a new system of records as defined in OMB Circular A-108, a systems notice must be published in the Federal Register and notices sent to OMB and both Houses of Congress as required by TM No. 1 of that Circular.

Document/Process No. 6

Matching
Report

Description: A matching report which meets all the requirements of the OMB Matching Guidelines is prepared by the matching agency. The report is then submitted to the Federal Register for publication, with formal copies of the report sent to OMB and both Houses of Congress.

OMB Matching Guidelines Reference: Paragraph 5.f.

Suggested Approach:

- Prepare the matching report, insuring that all requirements of the OMB Matching Guidelines are covered.
- Submit the report to the Federal Register for publication. It is preferable that this be done at least 30 days prior to the initiation of the match to allow those affected by the match to review the report and submit comments. A sample copy of a matching report as submitted for Federal Register publication is at Attachment G-1. Copies of matching reports as published in the Federal Register are at Attachment H.
- At the same time that the report is released for publication, copies must be sent to OMB and both houses of Congress. Copies of a transmittal letter (to the Speaker of the House) and a matching report as sent to OMB and Congress are at Attachment G-2.
- Comments received should be considered and modifications to the matching report made as necessary.

Document/Process No. 7

Obtain
Source
Agency
Data Files

Description: Once the source agency routine use notices are final, the source agency data files to be used in the match can be obtained. Since all data elements within the source agency files are not usually required, an extract of data essential to the match should be requested to limit the amount of data provided by a source agency.

OMB Matching Guidelines Reference: Paragraphs 5.a.(1), 5.b., 5.d.

Suggested Approach:

- Following the previously established procedures, the matching agency requests and receives source agency data files. Precise methodology for transferring data files to and from the matching agency should be covered in previous agreements between matching and source agencies.
- Matching agency stores and handles data files in accordance with Privacy Act provisions interagency agreements, and computer security requirements.
- Matching agency disposes of the data files by destruction or return to the source agencies as previously agreed upon.

Document/Process No. 8

Conduct
Computer
Matching

Description: The heart of the project, computer matching, involves file preparation, automated comparison of two or more files and selection of individual records based on pre-established criteria, automated purification and validation of selected records, and presentation of the resulting hit records in a form which can be used for followup actions. If necessary or beneficial, matches may be performed by outside organizations under contract to the matching agency.

OMB Matching Guidelines Reference: Paragraphs 5.c.(1), 5.d., 5.g.

Suggested Approach:

- If any of the data files to be matched are not in the proper format or specifications, reformat them so that they may be used.
- Produce and test the computer programs which will accomplish the matching.
- Perform the computer match, producing a file of "raw hits."
- Using available testing and purifying criteria, computer-validate the raw hits to the extent possible.
- Produce a set of hit records which can be referred to program staffs for further action.
- Store and/or dispose of the source agency data files as agreed upon.
- Store and control the file of hit records until no longer needed, then dispose of it as planned.

Document/Process No. 9

Analyze
and Refine
Raw Hits

Description: Matching agency program staffs receive the file of hits from computer matching. The staffs conduct such analyses and validations as necessary to insure the accuracy of the match data. The validating process should identify hits caused by program errors which need to receive different analysis from those caused by suspected program abuse. Prior to initiating any actions against identified individuals, the staffs should be reasonably sure that the individuals identified as hits are the same individuals suspected of program abuse. Close coordination with program staffs is essential when refining raw hits. Pursuing the hits is the most time-consuming and expensive phase of your match. The best purification of hits will lead to more successful results.

OMB Matching Guidelines Reference: Paragraphs 5.a.(1)(f), 5.c.(2), 5.d.(2)

Suggested Approach:

- Analyze hits to verify data with source agency or other program files, and try to determine: (1) if the individual identified by the match is the same individual suspected of program abuse, and (2) whether the hit is the result of program abuse or program error. For large matches, analysis of a sample of the hits might be used to assure integrity and validity of the matching process before embarking on extensive detailed analyses. This would include determination of the cause(s) of erroneous or excessive payments of benefits.

- Establish a file of validated hits for use in followup procedures.

- Destroy all match records of individuals eliminated from further consideration.

Document/Process No. 10

Perform Followup Procedures

Description: Followup activities include, but are not limited to: benefit payment terminations, debt and overpayment collections, program error corrections, and legal actions. The circumstances involved will dictate what followup procedures should be used for each matching project; however, followup procedures should parallel the followup process described in your match report. Corrective actions are, in most instances, the responsibility of program officials who administer the programs involved.

OMB Matching Guidelines Reference: Paragraphs 5.a.(1)(f), 5.d.(2), 5.f.(1)(f)

Suggested Approach:

- In cooperation with program staffs, verify abuse or identify error causes and initiate corrective measures. Eliminate or proceed very cautiously against any individual where doubt exists.
- Initiate administrative remedies including collection and recoupment actions in accordance with the Debt Collection Act of 1982 before considering civil court actions.
- When administrative remedies fail, initiate civil actions to recoup the funds due if appropriate.
- If criminal activity such as fraud is involved, initiate criminal action as appropriate.
- Institute a tracking system which will follow the various actions and monitor progress and effectiveness of the collection and litigation processes. This system should include accumulation of results for developing cost/benefit statistics.
- After completion of followup procedures, all records containing privacy data which are no longer required should be destroyed or returned to the sources of origin, as appropriate.

Attachment B

Systems of Records Notices

B1 VA

B2 OPM

58VA21/22/28

SYSTEM NAME:

Compensation, Pension, Education and Rehabilitation Records-VA.

SYSTEM LOCATION:

Records are maintained at the VA regional offices, the VA Records Processing Center, St. Louis, Missouri, and the Data Processing Center at Hines, Illinois, with subsidiary accounts receivable records located at the Data Processing Center, St. Paul, Minnesota. Active records are generally maintained by the regional office having jurisdiction over the domicile of the claimant. Address locations are listed in VA Appendix 1 at the end of this document.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The following categories of individuals will be covered by the system:

(1) Veterans who have applied for compensation for service-connected disability under 38 U.S.C. Chapter 11.

(2) Veterans who have applied for nonservice-connected disability, under 38 U.S.C. Chapter 23.

(3) Veterans entitled to burial benefits under 38 U.S.C. Chapter 15.

(4) Surviving spouses and children who have claimed pension based on nonservice-connected death of a veteran under 38 U.S.C. Chapter 15.

(5) Surviving spouses and children who have claimed pension based on service-connected death of a veteran under 38 U.S.C. Chapter 11.

(6) Surviving spouses and children who have claimed dependency and indemnity compensation for service-connected death of a veteran under 38 U.S.C. Chapter 13.

(7) Parents who have applied for death compensation based on service-connected death of a veteran under 38 U.S.C. Chapter 11.

(8) Parents who have applied for dependency and indemnity compensation for service-connected death of a vetaran under 38 U.S.C. Chapter 13.

(9) Veterans who have applied for VA educational benefits under 38 U.S.C. Chapters 31, 32 and 34.

(10) Spouses, surviving spouses and children of veterans who have applied for VA educational benefits under 38 U.S.C. Chapter 35.

(10) Spouses, surviving spouses and children of veterans who have applied for VA educational benefits under 38 U.S.C. Chapter 35.

(11) Servicemembers who have applied for educational benefits under 38 U.S.C. chapter 34 and 35.

(12) Servicemembers who have contributed money from their military pay to the post-Vietnam Era veterans Education Account under 38 U.S.C. Chapter 32.

CATEGORIES OF RECORDS IN THE SYSTEM:

The record, or information contained in the record, may include indentifying information (e.g., name, address, social security number); military service and active duty separation information (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, whether veteran was discharged with a disability, served in Vietnam Conflict, reenlisted, received a Purple Heart of other military decoration); payment information (e.g., veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments number of nonpaydays, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA); medical information (e.g., medical and dental treatment in the Armed Forces including type of service-connected disabilty, medical facilities or by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment); personal information (e.g., martial status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent's relationship to veteran); education benefit information (e.g., information arising from utilization or training benefits such as a veteran trainee's induction, reentrance or dismissal from a program or progress and attendance in an education or training program); applications for compensation, pension, education and rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, payment information, medical and dental information, personal and education benefit information relating to a veteran or beneficiary's incarceration in a penal institution (e.g., name of incarcerated veteran or beneficiary, claims file number, name and address of penal institution, date of commitment, type of offense, scheduled release date, vetreran's date of birth, beneficiary relationship to veteran and whether veteran or beneficiary is in a work release or half way house program, on parole or has been released from incarceration).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 38, United States Code, Chapter 3, section 210(c) and Chapters 11, 13, 15, 23, 31, 32, 34, 35, and 36.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. The record of an individual who is covered by this system may be disclosed to a member of Congress or staff person acting for the member when the member or staff person requests the record on behalf of and at the request of that individual.

2. Any information in this system may be disclosed to a Federal agency, upon its official request, to the extent that it is relevant and necessary to that agency's decision regarding: the hiring, retention or transfer of an employee; the issuance of a security clearance, the letting of a contract, or the issuance or continuance of a license, grant or other benefit given by that agency. However, in accordance with an agreement with the U.S. Postal Service, disclosures to the U.S. Postal Service for decisions concerning the employment of veterans will only be made with the veteran's prior written consent.

3. Any written information in this system may be disclosed to a State or local agency, upon official request, to the extent that it is relevant and necessary to that agency's decision on:

the hiring, retention or transfer of an employee, the issuance of a security clearance, the letting of a contract, or the issuance or continuance of a license, grant or other benefit by that agency: Provided, that if the information pertains to a veteran, the name and address of the veteran will not be disclosed unless the name and address is provided first by the requesting State or local agency.

4. Any information in this system, except for the name and address of a veteran, which is relevant to a suspected violation or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, may be disclosed to a Federal, State, local or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, rule, regulation or order issued pursuant thereto.

5. The name and address of a veteran, which is relevant to a suspected violation or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, may be disclosed to a Federal agency charged with the responsibility of investigation or prosecuting such violation or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto, in response to its official request.

6. The name and address of a veteran, which is relevant to a suspected violation or reasonably imminent violation of law concerning public health or safety, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, may be disclosed to any foreign, State or local governmental agency or instrumentality charged under applicable law with the protection of the public health or safety if a qualified representative of such organization, agency or instrumentality has made a written request that such name and address be provided for a purpose authorized by law.

7. The name and address of a veteran may be disclosed to any nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under title 38 U.S.C. (such disclosures include computerized lists of names and addresses).

8. Any information in this system, except for the name and address of a veteran, may be disclosed to a Federal agency in order for the VA to obtain information relevant to the issuance of a benefit under title 38 U.S.C. The name and address of a veteran may be disclosed to a Federal agency under this routine use if they are required by the Federal agency to respond to the VA inquiry.

9. Any information in this system may be disclosed in connection with any proceeding for the collection of an amount owed to the United States by virtue of a person's participation in any benefit program administered by the Veterans Administration when in the judgment of the Administrator, or official generally delegated such authority under standard agency delegation of authority rules (38 CFR 2.6), such disclosure is deemed necessary and proper, in accordance with 38 U.S.C. 3301(b)(6).

10. The name and address of a veteran, and other information as is reasonably necessary to identify such veteran, may be disclosed to a consumer reporting agency for the purpose of locating the veteran, or, obtaining a consumer report to determine the ability of the veteran to repay an indebtedness to the United States arising by virtue of the veteran's participation in a benefits program administered by the VA, provided that the requirements of 38 U.S.C. 3301(g)(2) have been met.

11. The name and address of a veteran, other information as is reasonably necessary to identify such veteran, and any information concerning the veteran's indebtedness to the United States by virtue of the person's participation in a benefits program administered by the VA may be disclosed to a consumer reporting agency for purposes of assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 3301(g)(4) have been met.

12. Any information in this system, including available identifying information regarding the debtor, such as name of debtor, last known address or debtor, VA insurance number, VA loan number, VA claim number, place of birth, date of birth of debtor, name and address of debtor's employer or firm and dates of employment may be disclosed, under this routine use, except to consumer reporting agencies, to a third party in order to obtain current name, address, locator, and credit report in connection with any proceeding for the collection of an amount owed to the United States by virtue of a person's participation in any VA benefit program when in the judgment of the Administrator such disclosure is deemed necessary and proper. This purpose is consistent with the Federal Claims Collection Act of 1966 (Public Law No. 89-508, 31 U.S.C. 951-953 and 4 CFR 101-105 and 38 U.S.C. 3301(b)(6)).

13. Any information in this system, including the nature and amount of a financial obligation, may be disclosed to a debtor's employing agency or commanding officer so that the debtor-employee may be counseled by his or her Federal employer or commanding officer and to assist in the collection of unpaid financial obligations owed the VA. This purpose is consistent with 5 U.S.C. 5514, 4 CFR 102.5, and section 206 of Executive Order 11222 of May 8, 1965 (30 FR 6469).

14. Payment information may be disclosed to the Department of the Treasury, in accordance with its official request, to permit delivery of benefit checks to veteran-payees.

15. Military service and active duty separation information, and identifying information may be disclosed to a State unemployment compensation agency to the extent required to determine eligibility for its benefits, provided the name and address of the individual to whom the record pertains are provided by the State agency. The purpose for this disclosure is consistent with 5 U.S.C. 8523.

16. Medical information may be disclosed in response to a request from the superintendent of a State hospital for psychotic patients, a commissioner or head of a State department of mental hygiene, or a head of a State, county or city health department or any fee basis physician or sharing institution in direct connection with authorized treatment for a veteran provided the name of the individual to whom the record pertains is given and the information will be treated as confidential, as is customary in civilian professional medical practice.

17. The name, branch of service, effective date of compensation, current and historical benefit pay amounts for disability or pension and the amount and type of education contribution made under title 38, United States Code, Chapter 32, may be disclosed to the following agencies upon their official request: Department of the Army, Navy, and Air Force; Department of Defense; Defense Manpower Data Center, Marine Corps; Department of Transportation (Coast Guard); Department of Health and Human Services; Department of Education; PHS (Public Health Service), NOAA (National Oceanic and Atmospheric Administration), Commissioned Officer Corps in order for these departments and agencies and the VA to reconcile the amount and/or waiver of service, department and retired pay.

18. The amount of pension, compensation, dependency and indemnity compensation, educational assistance allowance, retirement pay and subsistence allowance of any veteran identified to the VA may be disclosed to any person who applies for such information.

19. Identifying, personal, payment and medical information may be disclosed to a Federal, State, or local government agency at the request of a veteran in order to assist the veteran and insure that all of the title 38 U.S.C. or other benefits to which the veteran is entitled are received. This information may also be disclosed without a request from the veteran, to a Federal agency, upon its official request or to a State or local agency provided the name and address of the veteran is given beforehand by the State or local agency in order to assist the veteran in obtaining a non-title 38 U.S.C. benefit to which the veteran is entitled.

20. Any information in this system which directly affects payment or potential payment of benefits to contesting claimants, including parties claiming an apportioned share of benefits, may be coequally disclosed to each affected claimant upon request from that claimant in conjunction with the claim for benefits sought or received.

21. Any information in this system such as identifying information, nature of a claim, amount of benefit payments, percentage of disability and personal information, may be disclosed to the Social Security Administration, Bureau of Supplemental Security Income, upon its official request, in order for that agency to determine eligibility regarding amounts of social security benefits, or to verify other information with respect thereto.

22. Identifying information in this system may be disclosed at the request of a veteran to a third party having information relevant to a claim, such as an employer or school, in order to obtain information from the third party to the extent necessary to develop a veteran's claim for VA benefits.

23. Medical data (excluding the name and address of a veteran unless the name and address are furnished by the requestor) may be disclosed to epidemiological and other research facilities approved by the Chief Medical Director to obtain data from those facilities necessary to assist in medical studies on veterans for the Veterans Administration or for any research purposes determined to be necessary and proper by the Chief Medical Director.

24. The name(s) and address(es) of a veteran may be disclosed to another Federal agency or to a contractor of that agency, at the written request of the head of that agency or designee of the head of that agency for the purpose of conducting government research necessary to accomplish a statutory purpose of that agency.

25. Any information in this system relevant to a veteran's claim such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information and military service and active duty separation information may be disclosed at the request of the veteran to accredited service organizations, VA-approved claims agents and attorneys acting under a declaration of representation so that these individuals can aid veterans in the preparation, presentation and prosecution of claims under the laws administered by the VA. The name and address of a veteran will not, however, be disclosed to these individuals under this routine use if the veteran has not requested the assistance of an accredited service organization, claims agent or an attorney.

26. Identifying and payment information may be disclosed, upon the request of a Federal agency, to a State or local government agency, in order for that State or local government agency to determine a veteran's eligibility under programs provided for under Federal legislation and for which the requesting Federal agency has responsibility.

27. Any information in this system such as the amount of benefit or disability payments and medical information may be disclosed in the course of presenting evidence to a court, magistrate, or administrative authority, in matters of guardianship, inquests, and commitments, to private attorneys representing veterans rated incompetent in conjunction with issuance of Certificates of Incompetency, and to probation and parole officers in connection with court-required duties.

28. Any information in this system including medical information, the basis and nature of claim, the amount of benefits and personal information may be disclosed to a VA Federal fiduciary or a guardian ad litem in relation to his or her representation of a veteran only to the extent necessary to fulfill the duties of the VA Federal fiduciary or the guardian ad litem.

29. Any information in this system may be disclosed to the United States Department of Justice or United States Attorneys in order for the foregoing parties to prosecute or defend litigation involving or pertaining to the United States.

30. Any information in this system may be disclosed to a Federal grand jury, a Federal court or a party in litigation, or a Federal agency or party to an administrative proceeding being conducted by a Federal agency, in order for the VA to respond to and comply with the issuance of a Federal subpoena.

31. Any information in this system may be disclosed to a State or municipal grand jury, a State or municipal court or a party in litigation, or to a State or municipal administrative agency functioning in a quasi-judicial capacity or a party to a proceeding being conducted by such agency, in order for the VA to respond to and comply with the issuance of a State or municipal subpoena; provided, that any disclosure of claimant information made under this routine use must comply with the provisions of 38 CFR 1.511.

32. Any information in this system including the name, social security number, date of birth, delimiting date and remaining entitlement of VA educational benefits, may be disclosed to the ED (Department of Education), upon its official request, or contractor thereof, for specific use by the ED to validate information regarding entitlement to VA benefits which is submitted by applicants who request educational assistance grants from the ED. Such information will not be used for any other purpose by the ED or contractor thereof.

33. VA educational forms and letters which contain identifying information about a veteran may be disclosed at the request of the veteran to a VA-approved education or training establishment to assist the veteran in the completion of claims forms or for the VA to obtain further information from the educational or training establishments as may be necessary for the VA to properly process the veteran trainee's claim or to monitor the trainee's progress.

34. Identifying and payment information may be disclosed to a VA-approved educational or training establishment at the request of the veteran in order for the VA to obtain sufficient information necessary to pay the veteran or the educational or training establishment the correct monetary amounts in an expeditious manner. However, this information will not be provided under this routine use to an educational or training establishment when the request is clearly an attempt by that establishment to seek assistance in collection attempts against the veteran.

35. Identifying information and information regarding the induction, reentrance and dismissal of a disabled veteran from a vocational rehabilitation program may be disclosed at the request of the veteran to a VA-approved vocational rehabilitation training establishment to insure that the trainee receives the maximum benefit from training.

36. Identifying information and information regarding the extent and nature of a veteran's disabilities with respect to any limitations to be imposed on the veteran's vocational programs may be disclosed at the request of the veteran to a VA-approved vocational rehabilitation training establishment to insure that the trainee receives the maximum benefit from training.

37. Information regarding the type and amount of training/education received, and the name and address of a veteran, may be disclosed at the request of a veteran to local and State agencies and to prospective employers in order to assist the veteran in obtaining employment or further training.

38. The name, claims file number and any other information relating to a veteran's or beneficiary's incarceration in a penal institution and information regarding a dependent's right to a special apportionment of the incarcerated individual's VA benefit payment may be disclosed to those dependents who may be eligible for entitlement to such apportionment in accordance with 38 U.S.C. 504, 1682, 1780, and 3113.

39. The name, claims file number and any other information relating to a veteran or beneficiary who may be incarcerated in a penal institution may, pursuant to an arrangement, be disclosed to penal institutions or to correctional authorities in order to verify information concerning the veteran's or beneficiary's incarceration status. The disclosure of this information is necessary to determine that individual's continuing eligibility as authorized under 38 U.S.C. 504, 1682, 1780 and 3113.

40. Names and addresses, and other identifying data including the Social Security number, of surviving spouses, children and parents of decreased veterans may be released from this system of records to the Department of Defense (DOD) upon its official request in order for DOD to identify individuals eligible for health care benefits administered by the DOD, or to collect or verify information necessary for DOD facility planning, personnel studies, capitalization budgeting and post exchange, commissary and housing studies.

41. Identifying information including names and addresses, entitlement code, payee social security number, file number, payee number, regional office number, income for VA pension-determination purposes and pension net award may be released to the Department of Agriculture upon its official request for the purpose of a matching program designated USDA/OIG-6 for verification by the Department of Agriculture of applicants' eligibility for food stamps to reduce unauthorized payments in the food stamp program, and to collect debts owed to the United States Government. This anti-fraud matching program is being performed pursuant to the Department of Agriculture's Inspector General authority under Public Law No. 95-452, section 4(a), to detect and prevent fraud and abuse.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records (or information contained in records) are maintained on paper documents in claims file folders (e.g., "C" file folders, educational file folders and vocational rehabilitation file folders) and on automated storage media (e.g., microfilm, microfiche, magnetic tape and magnetic disks). Critical eligibility information regarding VA benefits is maintained on various automated storage media. Such information may be accessed through a data telecommunications terminal system denominated the Target System. Target terminal locations include VA Central Office, regional offices, and on a pilot basis some VA medical health care facilities. Information relating to receivable accounts owed to the VA, denominated the Centralized Accounts Receivable System (CARS), is maintained on magnetic tape and microfiche and microfilm. CARS is accessed through a data telecommunications terminal system at St. Paul, Minnesota.

RETRIEVABILITY:

Claims file folders are indexed by name of the veteran and VA file number. Automated records are indexed by named, VA file number, payee name and type of benefit.

SAFEGUARDS:

1. Physical Security: (a) access to working spaces and claims folder file storage areas in VA regional offices and centers is restricted to VA employees on a need-to-know basis. Generally, file areas are locked after normal duty hours and the offices and centers are protected from outside access by the Federal Protective Service or other security personnel. Employee claims file records and claims file records of public figures are stored in separate locked files. Strict control measures are enforced to ensure that access to and disclosure from these claims file records are limited to a need-to-know basis.

(b) Access to Target data telecommunications terminals is by authorization controlled by the site security officer. The security officer is assigned responsibility for privacy-security measures, especially for review of violations logs, information logs and control of password and badge distribution.

(c) Access to data processing centers is generally restricted to center employees, custodial personnel, Federal Protective Service and other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted.

2. Target System Security: (a) Usage of the Target terminal equipment is protected by key locks, magnetic badge readers and audible alarms. Electronic keyboard locks are activated on security errors.

(b) At the data processing centers, identification of magnetic tape and disks containing data is rigidly enforced using labeling techniques. Automated storage media which are not in use are stored in tape libraries which are secured in locked rooms. Access to programs is controlled at three levels: programming, auditing and operations.

RETENTION AND DISPOSAL:

Individual claims file folders and the compensation, pension, rehabilitation and education claims records contained therein are retained at the servicing regional office for the life of the veteran. At the death of the veteran, these records are sent to the Federal Records Center (FRC), maintained by the FRC for 75 years and thereafter destroyed. Rehabilitation and education counseling records are maintained until the exhaustion of a veteran's maximum entitlement or upon the exceeding of a veteran's delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is processed to determination. All other automated storage media is retained and disposed of in accordance with disposition authorization approved by the Archivist of the United States.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Compensation and Pension Service (21), Director, Education Service (22), Director, Vocational Rehabilitation and Counseling Service (28), VA Central Office, Washington, D.C. 20420.

NOTIFICATION PROCEDURE:

An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request or apply in person to the nearest Veterans Administration regional office or center. Address locations are listed in VA Appendix 1 at the end of this document.

RECORD ACCESS PROCEDURES:

Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest Veterans Administration regional office. Address locations are listed in VA Appendix 1 at the end of this document.

CONTESTING RECORD PROCEDURES:

(See Record access procedures above.)

RECORD SOURCE CATEGORIES:

The veteran, dependents and other beneficiaries of the veteran, accredited service organizations, VA-supervised fiduciaries (i.e., VA Federal fiduciaries, court-appointed fiduciaries), military service departments, VA medical facilities and physicians, private medical facilities and physicians, education and rehabilitation training establishments, State and local agencies, other Federal agencies, State, local and county courts and clerks, Federal, State and local penal institutions and correctional facilities, other third parties and other VA records.

[FR Doc. [illegible] Filed 1-4-82; 8:45 am]

BILLING CODE 8320-01-M

OPM/GOVT-1

SYSTEM NAME:

General Personnel Records.

SYSTEM LOCATION:

Records on current Federal employees are located at the Personnel Office or other designated office of the local installation of the Department or Agency which currently employs the individual. Where agencies determine that duplicates of these records need to be located in a second office, e.g., an administrative office closer to where the employee actually works, such copies are covered by this system. Former Federal employees' Official Personnel Folders (OPF) are located at the National Personnel Records Center, General Services Administration, 111 Winnebago Street, St. Louis, Missouri 63118. Records not considered long term records retained on the right-hand side of the OPF but which are also included in this system for former Federal employees, may be retained by agencies for a period of time after the employee leaves service.*

**The use of the phrase "long term" to describe right-hand side OPF records is used throughout since these records are not actually permanently retained. The term "temporary" is used when referencing left side OPF records and all other records covered by this notice.*

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former Federal employees as defined in 5 U.S.C. 2105.

CATEGORIES OF RECORDS IN THE SYSTEM:

Each category of record may include identifying information such as name(s), date of birth, home residence, mailing address, Social Security Number, and home telephone. This system includes, but is not limited to, the contents of the Official Personnel Folder as specified in Federal Personnel Manual Supplement 293-31. Records in this system include:

a. Records reflecting work experience, educational level achieved, and specialized education or training occurring outside of Federal service.

b. Records reflecting Federal service and documenting work experience and specialized education or training received while employed. Such records contain information about: past and present positions held; past and present grades, salaries, and duty station locations; commendations, awards, or other data reflecting special recognition of an employee's performance; and notices of all personnel actions such as: appointments, transfers, reassignments, details, promotions, demotions, reductions in force, resignations, separations, suspensions, Office approval of disability retirement applications, retirement and removals.

c. Records relating to enrollment or declination of enrollment in the Federal Employees Group Life Insurance Program and Federally-sponsored health benefit programs, as well as forms showing designation of beneficiary.

d. Records of a medical nature including records compiled during an agency-initiated fitness for duty examination or request for approval of disability retirement. Such medical records are to be retained in separate envelopes apart from the Official Personnel Folder (OPF) e.g., in the envelope that includes records of medical examinations that are to remain as long term records in the OPF (see "Retention and disposal" section below). (Note: this system does not cover agency dispensary records or records of drug or alcohol abuse counseling or other such counseling records.)

e. Records relating to an Intergovernmental Personnel Act assignment or Federal-private exchange program. (Note: some of these records may also become part of the OPM/CENTRAL-7, Intergovernmental Personnel Act Assignment Records, system.)

f. Records relating to participation in an agency Federal Executive or SES Candidate Development Program. (Note: some of these records may also become part of the OPM/CENTRAL-8, Federal Executive and SES Candidate Development Program Records, or OPM/CENTRAL-13, Senior Executive Service Records, systems.)

g. Records relating to Government-sponsored training or participation in an agency's Upward Mobility Program or other personnel programs designed to broaden an employee's work experiences and for purposes of advancement (e.g., and administrative intern program).

h. Records contained in the Central Personnel Data File (CPDF) maintained by the Office and exact representations thereof in agency manual or automated personnel information systems. These data elements include many of the above records along with handicap and race and national origin codes. A definitive list of CPDF data elements is contained in Federal Personnel Manual Supplement 292-1.

i. Records connected with the Senior Executive Service, maintained by agencies for use in making studies and analyses of the SES, preparing reports, and in making decisions affecting incumbents of these positions, e.g., relating to sabbatical leave programs, training, reassignments, and details, that are perhaps unique to the SES and which may or may not be filed in the employee's Official Personnel Folder. These records may also serve as basis for reports submitted to OPM's Executive Personnel and Management Development Group for purposes of implementing the Office's oversight responsibilities concerning the SES.

j. Records concerning an employee's activities on behalf of the labor organization representing agency employees, including accounting of official time spent and documentation in support of per diem and travel expenses. (Note: alternatively, such records may be retained by an agency payroll office, and thus subject to the agency's internal Privacy Act system of payroll records.)

k. Records that are performance-related, including: appraisal forms and supporting documentation issued under OPM approved employee (including SES employees) appraisal systems; recommendations for personnel actions; Performance Review Board or Executive Resource Board records; forms and supporting documentation issued in connection with removal actions; letters of commendation; and documents certifying satisfactory completion of probationary periods or recommendations for within grade or merit pay actions. Conduct-related records, such as reprimands, admonishments, cautions, or warnings and supporting documentation are also part of this system.

l. To the extent that the records listed here are also maintained in an agency automated personnel or microform records system, those versions of the above records are considered to be covered by this system notice. Any additional copies of these records (including performance appraisal and conduct-related documents maintained by first line supervisors and managers) maintained by agencies at field/administrative offices remote from where the original records exist are considered part of this system.

Note.—*It is not the intent of the Office to limit this system of records to the OPF only. Records may be filed in other folders which are located in Offices other than where the OPF is located. Further, as indicated in the records location section, some of these records may be duplicated for maintenance at a site closer to where the employee works (e.g., in an administrative office or supervisors work folder) and still be covered by this system.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 4308, 4315, 7504, 7514, 7543, 8347, 8716, 8913; and Executive Orders 9397, 9830, and 12107.

PURPOSE:

The Official Personnel folder (OPF) and other general personnel records files are the official repository of the records, reports of personnel actions, and the documents and papers required in connection with these actions effected during an employee's Federal service. The personnel action reports and other documents, some of which are filed as long term records in the OPF, give legal force and effect to personnel transactions and establish employee rights and benefits under pertinent laws and regulations governing Federal employment.

These files and records are maintained by agencies for the Office and in accordance with Office regulations and instructions. The Official Personnel Folder is maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage or, as appropriate, to the next employing agency. Other records are either retained at the agency for various lengths of time in accordance with General Services Administration records schedules or destroyed when they have served their purpose or when the employee leaves the agency. They provide the basic source of factual data about a person's Federal employment while in the service and after his or her separation. Records in this system have various uses by agency personnel offices, including: screening qualifications of employees; determining status, eligibility, and employee's rights and benefits under pertinent laws and regulations governing Federal employment; computing length of service; and for other information needed in providing personnel services. These records and their automated or microformed equivalents may also be used to locate individuals for personnel research.

Temporary documents on the left side of the OPF may lead (or have led) to a formal action, but do not constitute a record of it, nor make a substantial contribution to the employee's long term record.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records and information in these records may be used:

a. To disclose information to Government training facilities (Federal, State, and local) and to non-Government training facilities (private vendors of training courses or programs, private schools, etc.) for training purposes.

b. To disclose information to educational institutions on appointment of a recent graduate to a position in the Federal service, and to provide college and university officials with information about their students working under the Cooperative Education, Volunteer

Service, or other similar programs where necessary to a student's obtaining credit for the experience gained.

c. To disclose information to officials of foreign governments for clearance before a Federal employee is assigned to that country.

d. To disclose information to the Department of Labor, Veterans Administration, Social Security Administration, Department of Defense, Federal agencies that have special civilian employee retirement programs; or a national, State, county, municipal, or other publicly recognized charitable or Social Security Administration agency (e.g., State unemployment compensation agencies), where necessary to adjudicate a claim under the retirement, insurance or health benefits programs of the Office of Personnel Management or an agency cited above, or to an agency to conduct an analytical study or audit of benefits being paid under such programs.

e. To disclose to the Office of Federal Employees Group Life Insurance information necessary to verify election, declination, or waiver of regular and/or optional life insurance coverage or eligibility for payment of a claim for life insurance.

f. To disclose to health insurance carriers contracting with the Office of Personnel Management to provide a health benefits plan under the Federal Employees Health Benefits Program, information necessary to identify enrollment in a plan, to verify eligibility for payment of a claim for health benefits, or to carry out the coordination or audit of benefit provisions of such contracts.

g. To disclose information to a Federal, State, or local agency for determination of an individual's entitlement to benefits in connection with Federal Housing Administration programs.

h. To consider and select employees for incentive awards and other honors and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee awards or honors.

i. To consider employees for recognition through quality step increases, and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee recognition.

j. To disclose information to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

k. To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

l. To disclose information to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested), where necessary to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit.

m. To disclose to an agency in the executive, legislative, or judicial branch, or the District of Columbia Government in response to its request, or at the initiation of the agency maintaining the records, information in connection with the hiring of an employee; the issuance of a security clearance; the conducting of a security or suitability investigation of an individual; the classifying of jobs; the letting of a contract; the issuance of a license, grant, or other benefit by the requesting agency; or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision on the matter. (See 46 FR 3714, July 17, 1981.)

n. To disclose information to the Office of Management and Budget at any stage in the legislative coordination and clearance process in connection with private relief legislation as set forth in OMB Circular No. A–19.

o. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

p. To disclose information to another Federal agency or to a court when the Government is party to a judicial proceeding before the court.

q. By the National Archives and Records Service (General Services Administration) in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

r. By the agency maintaining the records or by the Office to locate individuals for personnel research or survey response, and in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related work force studies. While published statistics and studies do not contain individual identifiers, in some instances the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

s. To provide an official of another Federal agency information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected and maintained.

t. When an individual to whom a record pertains is mentally incompetent or under other legal disability, information in the individual's record may be disclosed to any person who is responsible for the care of the individual, to the extent necessary to assure payment of benefits to which the individual is entitled.

u. To disclose to the agency-appointed representative of an employee all notices, determinations, decisions, or other written communications issued to the employee, in connection with an examination ordered by the agency under:

(1) Fitness-for-duty examination procedures; or

(2) Agency-filed disability retirement procedures.

v. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.

w. To disclose to a requesting agency, organization, or individual the home address and other relevant information concerning those individuals who, it is reasonably believed, might have contracted an illness, been exposed to, or suffered from a health hazard while employed in the Federal work force.

x. To disclose specific civil service employment information required under law by the Department of Defense on individuals identified as members of the Ready Reserve, to assure continuous mobilization readiness of Ready Reserve units and members.

y. To disclose information to the Department of Defense, National Oceanic and Atmospheric Administration; United States Public Health Service, Veterans Administration, and the United States Coast Guard needed to effect any adjustments in retired or retained pay required by the dual compensation provisions of section 8332 of title 5, United States Code.

z. To disclose information to officials of the Merit Systems Protection Board, including the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of Office rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

aa. To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, examination of Federal affirmative employment programs, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures, or other functions vested in the Commission by the President's Reorganization Plan No. 1 of 1978.

bb. To disclose information to the Federal Labor Relations Authority (including its General Counsel) when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator's awards where a question of material fact is raised and matters before the Federal Service Impasses Panel.

cc. To disclose to prospective non-Federal employers, the following information about a current or former Federal employee:

(1) Tenure of employment;
(2) Civil service status;
(3) Length of service in the agency and the Government, and
(4) When separated, the date and nature of action as shown on the Notification of Personnel Action, Standard Form 50.

dd. To disclose information on employees of Federal health care facilities to private sector (i.e., other than Federal, State, or local government) agencies, boards, or commissions (e.g., the Joint Commission on Accreditation of Hospitals). Such disclosures will be made only where the disclosing agency determines that it is in the Government's best interest (e.g., to assist in the recruiting of staff in the community where the facility operates or to avoid any adverse publicity that may result from a public criticism of the facility's failure to obtain such approval) to obtain accreditation or other approval rating and only to the extent that the information disclosed is relevant and necessary for that purpose.

ee. To disclose information to any member of an agency's Performance Review Board or other board or panel (e.g., one convened to select or review nominees for awards of merit pay increases), when the member is not an official of the employing agency; information would then be used for the purposes of approving or recommending selection of candidates for executive development or SES candidate programs, issuing a performance appraisal rating, issuing performance awards, nominating for Meritorious and Distinguished Executive ranks, and removal, reduction-in-grade, and other personnel actions based on performance.

ff. To disclose information to the Federal Acquisition Institute (FAI) about Federal employees in procurement occupations and other occupations whose incumbents spend the predominant amount of their work hours on procurement tasks; provided that the FAI shall only use the data for such purposes and under such conditions as prescribed by the notice of the Federal Acquisition Personnel Information System as published in the Federal Register on February 7, 1980 (45 FR 8960). (See 46 FR 8[illegible]2, January 27, 1981.)

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

These records are maintained in file folders, on lists and forms, microfilm or microfiche, and in computer processible storage media.

RETRIEVABILITY:

These records are retrieved by various combinations of name, birth date, Social Security Number, or identification number of the individual on whom they are maintained.

SAFEGUARDS:

Paper or microfiched/microfilmed records are located in lockable metal file cabinets or in secured rooms with access limited to those personnel whose official duties require access. Access to computerized records is limited, through use of access codes and entry logs, to those whose official duties require access.

RETENTION AND DISPOSAL:

a. Long Terms, Records. The Official Personnel Folder (OPF) is retained by the employing agency as long as the individual is employed with that agency. Medical records are kept separate from the OPF while the individual is employed by an agency. When the individual transfers to another Federal agency or to another appointing office, the OPF, with the long term medical records, in a separate envelope, inserted therein is sent to that agency or office. Other medical records covered by this system, i.e., fitness for duty examinations, are considered temporary in nature. Such records, when not submitted to the Office for retention in a disability retirement file (or submitted, but the Office does not approve retirement), shall be destroyed no later than six months after closing action on the case, or sooner at the discretion of the agency.

Within 90 days after the individual separates from the Federal service, the OPF is sent to the National Personnel Records Center for long term storage. In the case of administrative need or a retired employee or one who dies in service, the OPF is sent to the Records Center within 120 days.

Destruction of the OPF is in accord with General Records Schedule 1.

b. Other Records. These records are detained for varying periods of time. Generally they are maintained for a minimum of one year, or until the employee transfers or separates.

c. Records contained on computer processible media with in the Central Personnel Data File (and in agency automated personnel records) may be retained indefinitely as a basis for longitudinal work history statistical studies.

SYSTEM MANAGER AND ADDRESS:

Assistant Director for Workforce Information, Compliance and Investigations Group, Office of Personnel Management, 1900 E. Street, N.W., Washington, D.C. 20415.

NOTIFICATION PROCEDURES:

Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or agency office, as follows:

a. Current Federal employees should contact the Personnel Officer or other responsible official (as designated by the employing agency), Department or Agency with which employed, Local Agency Installation, regarding records in this system.

b. Former Federal employees should contact one of the Office's regional or area offices (see list of regional office addresses in the Appendix), or, as explained in the Note Below, the National Personnel Records Center (Civilian), 111 Winnebago St., St. Louis, Missouri 63118, regarding the records in this system.

Individuals must furnish the following information for their records to be located and identified:

a. Full name.

b. Date of birth.

c. Social Security Number.

d. Last employing agency (including duty station) and approximate date of the employment (for former Federal employees).

e. Signature

RECORD ACCESS PROCEDURES:

Individuals wishing to request access to their records should contact the appropriate OPM or agency office, as specified in the Notification procedures section. Individuals must furnish the following information for their records to be located and identified:

a. Full name.

b. Date of birth.

c. Social Security Number.

d. Last employing agency (including duty station) and approximate date of the employment (for former Federal employees).

e. Signature.

Individuals requesting access must also comply with the Office's Privacy Act regulations regarding verification of identity and access to records (5 CFR 297.201 and 297.203).

Note.—An individual who is a former Federal employee may direct a request to the National Personnel Records Center (NPRC) for a copy of a specific OPF document or for a transcript of his or her own employment history compiled from documents in the Offical Personnel Folder (OPF). The transcript includes the individual's name; date of birth; Social Security Number; past and present grades, position titles, duty stations, and salaries; and dates of personnel actions.

Under no circumstances shall an individual direct a request to NPRC for access to copies of all records maintained in his/her OPF. Though NPRC stores and services the OPFs of former Federal employees covered by this system that record remains the property of the Office of Personnel Management, and such requests will be handled and processed by the nearest OPM office to where the requester lives. (See list of OPM regional office addresses in the Appendix.)

CONTESTING RECORD PROCEDURES:

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager and not the nearest OPM office. Individuals must furnish the following information for their records to be located and identified:

a. Full name.

b. Date of birth.

c. Social Security Number.

d. Last employing agency (including duty station) and approximate dates of the employment (for former Federal employees).

e. Signature.

Individuals requesting amendment must also comply with the Office's Privacy Act regulations regarding verification of identity and amendment of records (5 CFR 297.201 and 297.208).

Note.—Under no circumstances shall former employees direct a request for amendment to records in the OPF to the NPRC or to OPM regional or area offices. NPRC only stores and services the OPFs on former Federal employees covered by this system and OPM regional or area offices process only access requests. Processing under the amendment provisions of the Privacy Act will be handled only by the system manager.

RECORD SOURCE CATEGORIES:

Information in this system of records is provided by:

a. The individual on whom the record is maintained.

b. Physicians examining the individual.

c. Educational institutions.

d. Agency officials and other individuals or entities.

e. Other sources of information for long term records maintained in an employee's OPF, in accordance with Federal Personnel Manual Chapter 293.

Attachment C

HHS Notice of Intent to Establish a System of Records

Privacy Act of 1974; Report on New System

AGENCY: Health and Human Services Department.

ACTION: Notification of Report on New System, "Federal Personnel/HHS or HHS Funded Benefit and Loan Program Temporary Matching File, HHS/OS/OIG".

SUMMARY: The Department of Health and Human Services proposes to establish a new system of records entitled "Federal Personnel/HHS or HHS-Funded Benefit and Loan Program Temporary Matching File, HHS/OS/OIG", under the Privacy Act and in accordance with OMB Supplemental Guidance for Matching Programs. The Department is requesting public comments on the routine uses in the system.

DATES: The Department has sent new system reports for this system to the Congress and OMB on August 13, 1982. The Department has requested a waiver of the 60 day advance notification required by OMB Circular A-108. If this waiver is granted, the systems notice, with the exception of the routine uses, will be effective on the date the waiver is granted. Regardless of whether a waiver is granted, the routine uses will not be effective before 30 days from the date of publication provided no comment is received which results in a contrary determination. If the waiver is not granted, the systems notice will be effective 60 days from the date submitted to OMB.

ADDRESS: Comments should be addressed to Richard McGowan, Public Affairs Officer, Office of Inspector General, Department of Health and Human Services, Room 5287 North Bldg., 330 Independence Avenue, SW., Washington, D.C. 20201. Comments received will be available for inspection at the above address.

FOR FURTHER INFORMATION CONTACT: Mr. Richard McGowan, Public Affairs Officer, Office of the Inspector General, Department of Health and Human Services, at the above address or call (202) 472-3142.

SUPPLEMENTARY INFORMATION: The Office of Inspector General under the auspices of the President's Council on Integrity and Efficiency has initiated a major project to reduce fraud and abuse by federal employees, retirees, or survivors who are improperly receiving federal or federally funded benefits or who have debts owing to the federal government and to identify program weaknesses requiring corrective action. The project will consist of matches of federal personnel records against HHS or HHS funded program records to identify individuals who appear in both records systems. Cases identified through computer comparison of files will be forwarded to the federal employing agency for verification of status. Cases will then be referred to the appropriate federal, state, or local agency for an entitlement determination or collection of outstanding debts. Where there is evidence of fraud, cases will be referred to the appropriate federal, state, or local law enforcement agency for investigation and prosecution. It is expected that federal employing agencies will pursue administrative sanctions in appropriate cases.

The routine use disclosures provided for in the notice are necessary to accomplish the purposes of the system of records as described above or are compatible with the collection of data for those purposes. Disclosures will also be made in accordance with other disclosure provisions of the Privacy Act (5 U.S.C. 552a(b)).

Dated: August 13, 1982.

Richard P. Kusserow,

Inspector General.

[illegible]

SYSTEM NAME:

Federal Personnel/HHS or HHS Funded Benefit and Loan Program Temporary Matching File HHS/OS/OIG.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Office of the Inspector General, DHHS, Room 5282, North Building, 330 Independence Avenue, SW., Washington, D.C. 20201.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Federal personnel (employees, retirees, and survivors) who are also included in HHS or HHS funded benefit and loan program record files.

CATEGORIES OF RECORDS IN THE SYSTEM:

Federal personnel records including name, social security number, date of birth, sex, work status, pay grade, duty station, OPM claim number, health benefit enrollment code, retirement date, annuity rate, pay status of case, correspondence address, zip code, and HHS or HHS funded benefit and loan program records including name, social security number, date of birth, address, and data used to determine eligibility.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Pub. L. 94-505.

PURPOSE(S):

This system of records is maintained to facilitate the comparison of records to identify those federal employees, federal retirees, or their survivors who may also be receiving assistance under an HHS or HHS funded benefit or loan program. These records will then be used for the purpose of reviewing eligibility and identifying any debts owed under these programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records may be used as follows:

1. In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, foreign, State or local, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto where such responsibility rests outside of OIC.

2. A record from this system of records may be disclosed as a "routine use" to a Federal, State or local agency maintaining civil, criminal or other relevant enforcement records or other pertinent records, such as current licenses, if necessary to obtain a record relevant to an agency decision concerning the hiring or retention of an employee or disciplinary or other administrative action concerning an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

3. A record from this system of records may be disclosed to a Federal agency in connection with the hiring or retention of an employee or disciplinary or other administrative action concerning an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the agency, to the extent that the record is relevant and necessary to the agency's decision on the matter.

4. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

5. In the event of litigation where the defendant is (a) the Department, any component of the Department, or any employee of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the department or any of its components; or (C) any Department employee in his or her individual capacity where the Justice Department has agreed to represent such employee, the Department may disclose such records as it deems desirable or necessary to the Department of Justice to enable that Department to effectively represent such party, provided such disclosure is compatible with the purpose for which the records were collected.

6. A record from this system may be disclosed as a "routine use" to a Federal, State, or local agency maintaining pertinent records if necessary to obtain a record relevant to a Department decision concerning the determination of initial or continuing eligibility for program benefits.

7. Disclosures may be made to the Office of Personnel Management or the Merit Systems Protection Board (including the Office of the Special Counsel) of information relevant and necessary to carrying out their functions.

8. Disclosures may be made to third party contacts where the party contacted may have information needed to establish or verify relevant information.

9. Disclosures may be made to Federal, State, and local agencies or to other agencies administrating federally funded programs where necessary to take action with regard to individuals not entitled to program benefits or individuals delinquent on loan payments under federally funded programs.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

The records are stored on computer tape files and computer printed listings.

RETRIEVABILITY:

The records are retrieved by computer using Social Security Number as the principal matching criterion.

SAFEGUARDS:

Direct access is restricted to authorized staff members of the Office of the Inspector General. Access within HHS is limited to those employees who are directly involved in the matching program on a need-to-know basis. Computer files and printed listing are maintained in security type safes or lock bar file cabinets. They are safeguarded in accordance with the provisions of the National Bureau of Standards Federal Information Processing Standards 41 and 31, and the HHS Information Processing Standards, HHS ADP Systems Manual, Part 6, "ADP Systems Security." All computer tapes are password protected prohibiting unauthorized access.

RETENTION AND DISPOSAL:

In instances of computer matching of files, only those records which meet predetermined criteria are maintained. All records which do not meet these criteria are destroyed. All original source commuter tapes will be returned within 60 days. All records obtained as a result of the matching program will be degaussed as soon as possible within 6 months except for those records which are necessary to the completion of pending law enforcement activities or administrative activities of the matching program. Paper listings will be either shredded or burned.

SYSTEM MANAGER(S) AND ADDRESS:

Inspector General/Deputy Inspector General, Room 5246, North Building, U.S. Department of Health and Human Services, 330 Independence Avenue, SW., Washington, D.C. 20201.

NOTIFICATION PROCEDURE:

Contact: Richard McGowan, Public Affairs Officer, Office of Inspector General, Department of Health and Human Services, Room 5287, North Building, 330 Independence Avenue, SW., Washington, D.C. 20201.

RECORD ACCESS PROCEDURES:

Same as notification procedure. Requesters should also reasonably specify the record contents being sought.

CONTESTING RECORD PROCEDURES:

Contact the official at the address specified under notification procedure above, and reasonably identify the record and specify the information to be contested, the corrective action sought and the reasons for the correction with supporting justification.

RECORD SOURCE CATEGORIES:

Records are furnished from the Central Personnel Data File (CPDF) maintained by the Office of Personnel Management, from other Federal agency personnel records systems, and from HHS or HHS-funded program records systems.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None

[FR Doc. [illegible] Filed [illegible]]

BILLING CODE [illegible]

Attachment D

Source Agency Data File Format and Specifications

FEDERAL PERSONNEL INDEBTED TO THE VA - MATCHING PROGRAM
MATCHING SOURCE PERSONNEL DATA EXTRACT FORMAT

PROVIDER PERSONNEL DATA EXTRACT					
DATA ELEMENT NUMBER	DATA ELEMENT TITLE	TAPE POSI-TION	ELEMENT LENGTH & TYPE	DATA ELEMENT DESCRIPTION	DEFAULT ENTRY
1	Category of Individual	000-001	2 A	Provider-entered code identifying the category of individual in the file: Civil Svc Employees CA Civil Svc Annuitants CR Civil Svc Primary Survivors CS Civil Svc Surviving Children CC DOD Active Duty Military AA DOD Retired Military AR DOD Military Reservists AF DOD Primary Survivors AS DOD Surviving Children AC TVA Employees TA TVA Annuitants TR USCG Active Duty Military GA USCG Military Reservists GF USCG Military Retirees GR US Post Office Employees PA	None
2	Social Security Number	002-010	9 A/N	Self-explanatory. Enter whatever appears in SSN field of source record.	None
3	Social Security Number Suffix	011	1 A/N	Enter if applicable.	Blank
4	Date of Birth	012-017	6 N	Enter standard date (YYMMDD). If year not available, enter all zeros. Enter year or year and month if full date not available and zero-fill the remainder of this field.	Zeros
5	Sex	018	1 A	Enter "M" for Male or "F" for Female. For Category CR, CS, and CC records, enter "M" for source record codes 1, 3, or 5; or "F" for source record codes 2, 4, or 6.	Blank
6	Name	019-048	30 A/N	Enter Last Name, then First Name, then Middl Initial. Left justify Last Name and blank-fill remainder of field.	Blanks

PROVIDER PERSONNEL DATA EXTRACT (Cont'd) Page 2

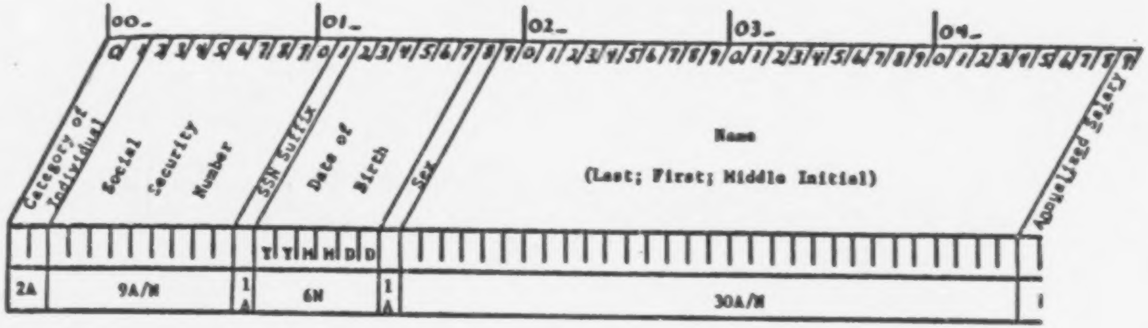
DATA ELEMENT NUMBER	DATA ELEMENT TITLE	TAPE POSI-TION	ELEMENT LENGTH & TYPE	DATA ELEMENT DESCRIPTION	DEFAULT ENTRY
7	Annualized Salary	049-053	5 N	Enter whole-number annual salary. Periodic salaries must be annualized before entering. Right-justify and zero-fill this field. Enter all zeros if annualized salary is not available or cannot be determined.	Zeros
8	Service Computation Date or Basic Active Service Date	054-059	6 N	Enter standard date, if available, for current employees only. See element #4 for handling of partial dates.	Zeros
9	Separation/Retirement Date	060-065	6 N	Enter standard date if applicable. See element #4 for handling of partial dates.	Zeros
10*	Reportable Handicap	066-067	2 N	See pages III-25 thru 27, FPM Suppl 292-1, for description of entries.	Zeros
11*	Veteran's Preference Code	068	1 N	See page III-135, FPM Suppl 292-1.	Zero
12*	Retirement Code	069	1 N	See page III-122, FPM Suppl 292-1.	Zero
13*	Occupation Code	070-074	5 N	See pages III-47 thru 95, FPM Suppl 292-1.	Zeros
14*	Position Occupied	075	1 N	See page III-119, FPM Suppl 292-1.	Zero
15*	Work Schedule Code	076	1 A	See page III-136, FPM Suppl 292-1.	Blank
16*	Agency Code	077-078	2 A/N	See pages III-96 thru 107, FPM Suppl 292-1.	Blanks
17*	Agency Subelement Code	079-080	2 A/N	Same as for element #16.	Blanks
18*	Geographic Location Code	081-089	9 A/N	See GSA publication, "Worldwide Geographic Codes" dated Nov 76, as amended by FPM Bulletin 290-20, May 79.	Blanks
19*	S.M.S.A.	090-093	4 A/N	Standard Metropolitan Service Area code from the Census Bureau. Permits grouping individuals within metropolitan population centers.	Blanks
20*	Special Program Identifier	094-095	2 N	See page III-125, FPM Suppl 292-1.	Zeros
21*	Submitting Office Number (SON)	096-099	4 N	Identifies personnel office which submitted source data to OPM. Mag tape of SON's and office identifications and locations is available from OPM.	Zeros
- * -	Elements 10 thru 21 are for OPM Records, Category CA, only. For all other categories, enter default.				
22	Pay Status of Case	100	1 A/N	OPM use only. For Cat CR, CS, & CC only.	Blank
23	OPM Claim Number	101-109	9 A/N	OPM use only. For Cat CR, CS, & CC only.	Blank
24	Health Benefit Enrollment Code	110-112	3 A/N	Identifies the Health Benefit Plan for Civil Svc Annuitants and Survivors. Cat CR, CS, CC	Blanks

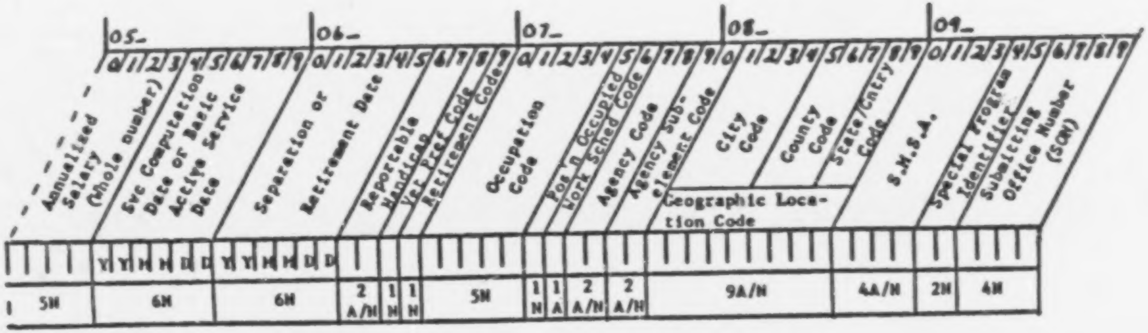
PROVIDER PERSONNEL DATA EXTRACT (Concluded) Page 3

DATA ELEMENT NUMBER	DATA ELEMENT TITLE	TAPE POSI-TION	ELEMENT LENGTH & TYPE	DATA ELEMENT DESCRIPTION	DEFAULT ENTRY
25	Date of Death	113-118	6 A/N	Enter standard date if applicable. For Civil Svc Annuitants: if Pay Status Code is "J" and Current Pay Action Code is "P01", enter Pay Action Change Effective Date in this field.	Zeros
26	ZIP Code	119-123	5 A/N	If contact (mail or office) ZIP Code is separately available, enter here as well as in the Contact Address field, element #29.	Blanks
27	Veterans Administration Claim Number	124-132	9 A/N	Enter, if available.	Blanks
28	Social Security Number Valid	133	1 A	If SSN has been validated, enter "Y"; if not, enter "N".	"N"
29	Contact Address	134-265	132 A/N	Enter: mailing/correspondence address; organizational address; or other contact address, if available. An entry in this field should provide the Matching Agency an address through which the individual can be contacted.	Blanks
30	"As Of" Date of File	266-269	4 N	Standard (YYMM) month and year indicating latest update of the source file(s). The last day of the month shown will be the presumed "as of" day for this field.	None

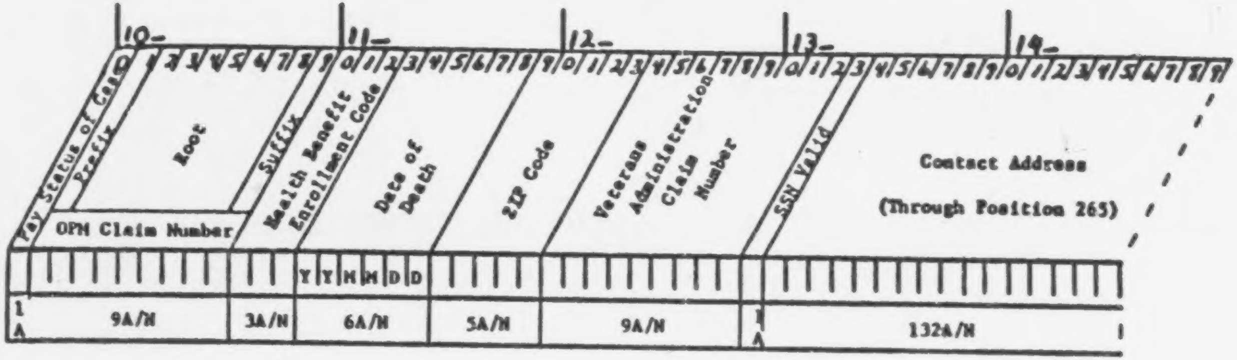
PROVIDER PERSONNEL DATA EXTRACT

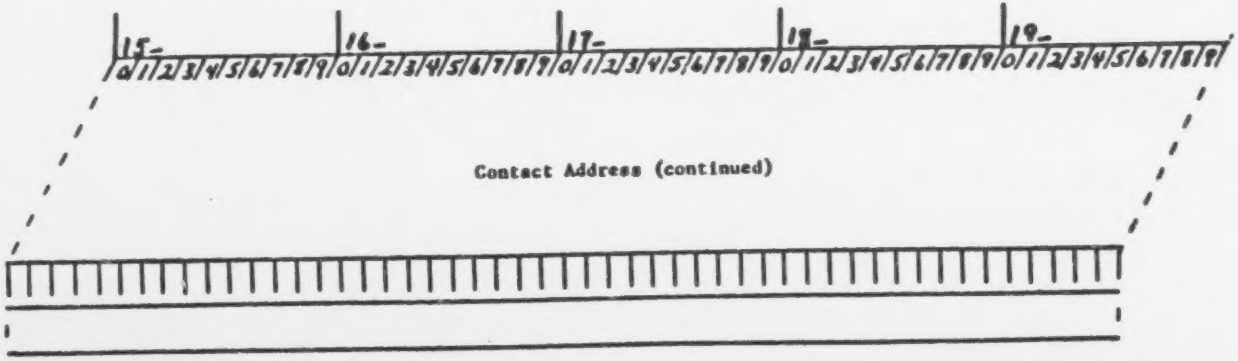
Page 4

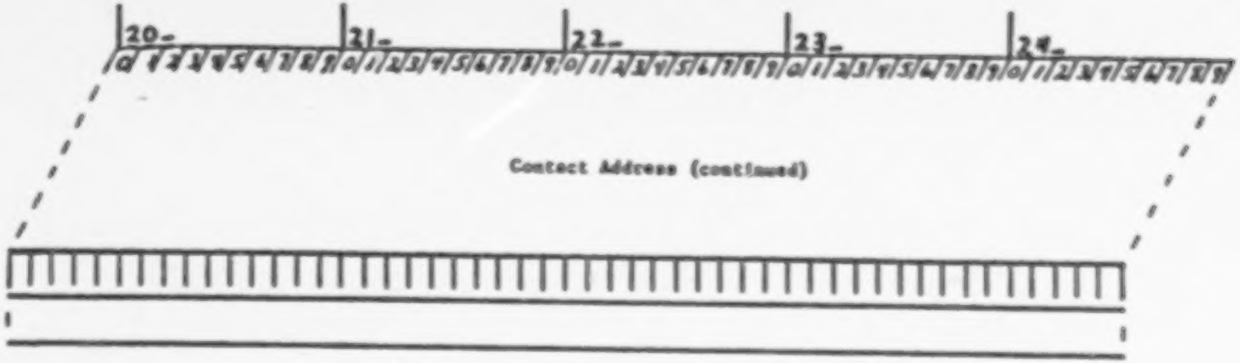

00_
01_
02_
03_
04_
Category of Individual
Social Security Number
SSN Suffix
Date of Birth
Sex
Name
(Last; First; Middle Initial)
Annualized Salary
Y Y M M D D
2A
9A/N
1 A
6N
1 A
30A/N
1

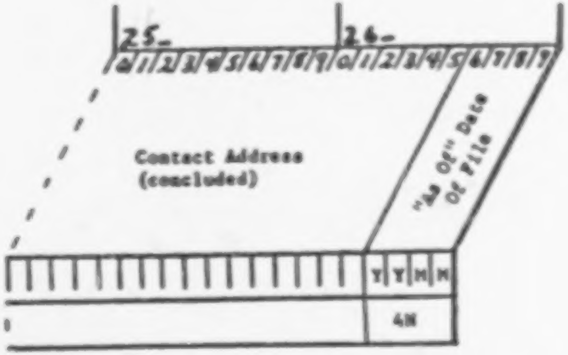

05_
06_
07_
08_
09_
Annualized Salary (Whole number)
Svc Computation Date or Basic Active Service Date
Separation or Retirement Date
Reportable Handicap
Vet Pref Code
Retirement Code
Occupation Code
Pos'n Occupied
Work Sched Code
Agency Code
Agency Sub-element Code
City Code
County Code
State/Cntry Code
Geographic Location Code
S.M.S.A.
Special Program Identifier
Submitting Office Number (SON)
Y Y M M D D
Y Y M M D D
1
5N
6N
6N
2 A/N
1 N
1 N
5N
1 N
1 A
2 A/N
2 A/N
9A/N
4A/N
2N
4N

PROVIDER PERSONNEL DATA EXTRACT (Cont'd).


10-
11-
12-
13-
14-
Pay Status of Case
Prefix
Root
Suffix
OPM Claim Number
Health Benefit Enrollment Code
Date of Death
ZIP Code
Veterans Administration Claim Number
SSN Valid
Contact Address
(Through Position 265)
Y Y M M D D
1 A
9A/N
3A/N
6A/N
5A/N
9A/N
1 A
132A/N


15-
16-
17-
18-
19-
Contact Address (continued)


20-
21-
22-
23-
24-
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
Contact Address (continued)


25-
26-
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
Contact Address (concluded)
"As Of" Date Of File
Y Y M M
4N

Tape Specifications:
Record length: 270 bytes
Blocking factor: 50 records/block
Tracks: 9; Parity: Odd; Unlabeled
EBCDIC; Display mode; Unsigned
Recording density: 6250 bpi
(1600 bpi is acceptable)

Attachment E

Source Agency Routine Use Notices

E1	HHS
E2	OPM

Office of the Secretary

Privacy Act of 1974; Proposed Amendment to System of Records

AGENCY: Office of the Assistant Secretary for Personnel Administration, Office of the Secretary, HHS.

ACTION: Notice of proposed new routine uses for existing system of record.

SUMMARY: The Department is giving notice that it intends to add two new routine uses to the following Privacy Act record system notice: 09-90-0017—Pay, Leave, and Attendance Records, HHS/OS/ASPER. Records in this system of records are used to insure that each employee receives the proper pay and allowances; that proper deductions and authorized allotments are made from employees' pay; that employees are credited and charged with the proper amount of sick and annual leave; and to enforce employee responsibilities through such actions as income tax levies, garnishments for child support/alimony, and deductions for the payment of debts owed the United States. We invite public comment on these new routine use disclosures (numbers 18 and 19 in notice below).

EFFECTIVE DATE: This amendment shall become effective without further notice June 17, 1983, unless comments are received on or before that date which would result in a contrary determination.

ADDRESS: Comments should be address to: Director, Division of Policy, Room 2316 Switzer Building, 300 C Street, S.W., Washington D.C. 20201.

FOR FURTHER INFORMATION CONTACT: Jim Wormley, OASPER, Division of Policy, telephone: 202-245-1984.

SUPPLEMENTARY INFORMATION: The U.S. Department of Labor (DOL), Office of the Inspector General, has asked the U.S. Department of Health and Human Services (HHS) for certain information applicable to every HHS employee that was paid during pay periods ending between October 3, 1981 and October 2, 1982 inclusive. The DOL has made the request because they are conducting, under the auspices of the President's Council on Integrity and Efficiency, a computerized crossmatch to identify HHS employees who have drawn unemployment benefits in violation of unemployment insurance laws. The data items which DOL is requesting are as follows: Social Security Number, employee name, agency code, agency sub-element/Division code, geographic location code, record length, pay period beginning date, pay period ending date, number of hours/days worked during the pay period, and gross pay. With two exceptions, Social Security account number and number of hours/days worked per pay period, the information requested by DOL is public information under 5 CFR 294.702. The purpose of the DOL computerized matching program is to reduce fraud and abuse in State unemployment compensation programs. HHS is serving as a matching source agency in this DOL anti-fraud matching program. As such, HHS has made the determinations required for source agencies by the Office of Management and Budget Guidelines for the Conduct of Matching Program.

The U.S. Department of Agriculture (USDA), Office of the Inspector General, has asked HHS for certain wage information on a single HHS employee. The information, which will be used to confirm eligibility, is needed in conjunction with a USDA audit of the Food Stamp Program in Fulton County, Georgia. A purpose of this audit, and all audits of loan and benefit programs performed by USDA and other Federal Agencies, is to reduce fraud and abuse in the administration of these programs.

The propose of this notice is to establish the routine uses required for the Privacy Act record system from which information will be provided to the DOL and the USDA (numbers 18 and 19 in the notice below) under the circumstances described above and to other Federal agencies under similar circumstances in the future.

The Privacy Act allows disclosure of information under a routine use for purposes that are compatible with the purposes for which the information was collected. Disclosure under these proposed routine uses will assist Federal agencies in their efforts to eliminate fraud, waste and abuse in loan and benefit programs they administer and in State and local programs over which they have cognizance. This goal is compatible with the OASPER functional responsibility for oversight of HHS employees' conduct, particularly with the requirement that employees conduct themselves in a proper manner, not obtain financial benefits in a fradulent manner, and pay their just obligations (see the HHS Standards of Conduct regulations in 45 Code of Federal Regulations Part 735). This responsibility is appropriately achieved through the use of this record system which is used to enforce these employee responsibilities through actions such as income tax levies, garnishments for child support/alimony, and deductions for the payment of debts owed the United States

Routine use number 17 was inadvertently omitted from the last publication of this notice in Federal Register, Volume 47, Number 198, October 13, 1982, pages 45759-45761. That routine use was added to this record system notice in Federal Register, Volume 47, Number 70, April 12, 1982, pages 15647-15650. This notice also updates the organizations and addresses of Payroll Liaison Officers in Appendix 1 of the record system notice.

A notice will be issued annually informing employees that these records may be disclosed to Federal agencies for the purpose of conducting computer matching programs designed to eliminate fraud, waste and abuse in loan and benefit programs.

May 11, 1983.

Thomas S. McFee,

Assistant Secretary for Personnel Administration.

SYSTEM NAME:

Pay, Leave and Attendance Records, HHS/OS/ASPER.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Pay Systems Division, Department of Health and Human Services, 330 Independence Avenue SW., Washington, D.C. 20201.

Payroll Liaison Representatives. See Appendix 1. Timekeepers in organizational units serviced by Payroll Liaison Representatives shown in Appendix 1. Personnel offices shown in HHS System 09900008, Applicants for Employment Records, Appendix 1.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

All paid employees of the Department of Health and Human Services including PHS Commissioned Corps Personnel.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system consists of a variety of records relating to pay and leave determinations made about each employee of the Department of Health and Human Services. In addition to the name of the employee, the system includes information such as the employee's date of birth, social security number, home address, grade or rank, employing organization, timekeeper number, salary, Civil Service retirement fund contributions, pay plan, number of hours worked, annual and sick leave accrual rate and usage, annual and sick leave balance, FICA withholdings, Federal, state and city tax withholdings, Federal Employees Governmental Life Insurance withholdings, Federal Employees Health Benefits withholdings, garnishment documents, savings allotments, union and management association dues withholdings allotments, savings bonds allotments, and Combined Federal Campaign allotments; for Commissioned Corps Personnel, information such as the following is included: years of service, payroll number, base pay, incentive pay, hazardous pay, allowances and Servicemen's Group Life Insurance.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 5501 et seq., 5525 et seq., 5301 et seq.; 42 U.S.C. 201 et seq., and Pub. L. 93-63.

PURPOSE(S):

Records in this system are used to insure that each employee receives the proper pay and allowances; that proper reductions and authorized allotments are made from employees' pay; and that employees are credited and charged with the proper amount of sick and annual leave. These records are maintained in each component of the Department. See also "Retrievability" below.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Information in this system of records is used or may be used:

(1) To prepare W-2 Forms to submit to the Internal Revenue Service and to disclose to state and local government agencies having taxing authority pertinent records relating to employees, including name, home address, social security number (in accordance with Section 7 of Pub. L. 93-579), earned income, and amount of taxes withheld.

(2) In the event that this system of records indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

(3) A record from this system of records may be disclosed as a "routine use" to a federal, state or local agency maintaining civil, criminal or other relevant enforcement records or other pertinent records, such as current licenses, if necessary to obtain a record relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant or other benefit.

A record from this system of records may be disclosed to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the record is relevant and necessary to the requesting agency's decision on the matter.

(4) In the event that this system of records indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use to the appropriate agency, whether state or local charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.

(5) Where federal agencies having the power to subpoena other federal agencies' records, such as the Internal Revenue Service or the Civil Rights Commission, issue a subpoena to the Department for records in this system of records, the Department will make such records available.

(6) Where a contract between a component of the Department and a labor organization recognized under E.O. 11491 or 5 U.S.C. Chapter 71 provides that the agency will disclose personal records relevant to the organization's mission, records in this system of records may be disclosed to such organization.

(7) The Department contemplates that it will contract with a private firm for the purpose of collating, analyzing, aggregating or otherwise refining records in this system. Relevant records will be disclosed to such a contractor. The contractor shall be required to maintain Privacy Act safeguards with respect to such records.

(8) By the Office of Personnel Management, Merit Systems Protection Board (including its Office of the Special Counsel), Equal Employment Opportunity Commission, and the Federal Labor Relations Authority (including the General Counsel of the Authority and the Federal Service Impasses Panel) in carrying out their functions.

(9) By the Department of Labor to make compensation determination in connection with a claim filed by the employee for compensation on account of a job-connected injury or disease.

(10) To respond to court orders for garnishment of an employee's pay for alimony or child support.

(11) To respond to orders from IRS for garnishment of an employee's pay for Federal income tax purposes.

(12) To the Department of Treasury for the purposes of preparing and issuing employee salary and compensation checks and U.S. Savings Bonds.

(13) By state officers of unemployment compensation in connection with claims filed by former HHS employees for unemployment compensation.

(14) Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

(15) In the event of litigation where the defendant is (a) the Department, any component of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the Department of any of its components; or (c) any Department employee in his or her individual capacity where the Justice Department has agreed to represent such employee, the Department may disclose such records as it deems desirable or necessary to the Department of Justice to enable that Department to present an effective defense, provided such disclosure is compatible with the purpose for which the records were collected.

(16) By financial organizations designate to receive labor organization or management association dues withheld from employee's pay, in order to account for the amounts of such withheld dues which they receive.

(17) A record from this system of records may be disclosed to a State or local agency for the purpose of conducting computer matching programs designed to reduce fraud, waste and abuse in Federal, State and local public assistance programs and operations.

(18) A record from this system of records may be disclosed to a Federal agency for the purpose of conducting computer matching programs designed to reduce fraud, waste and abuse using loan or benefit records of a Federal, State or local agency to identify employees improperly receiving loans or benefits and to facilitate the collection of debts owed the United States.

(19) A record from this system of records may be disclosed to a Federal agency in response to a written request from that agency, personally signed by a supervisor, specifying the particular portion desired and the law enforcement activity for which the record is sought. The request for the record must be connected with the agency's auditing and investigative functions designed to reduce fraud, waste and abuse; it must be based on information which raises questions about an individual's eligibility for benefits or payments; and it must be made reasonably soon after the information is received.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Magnetic tape, microfilm, punch cards and forms.

RETRIEVABILITY:

Records are maintained by pay period and are retrievable by name, SSN and Timekeeper number within each pay period. Records are also used to produce summary descriptive statistics and analytical studies in support of the functions for which the records are collected and maintained and for related personnel management functions or pay studies, and for other purposes compatible with the intent for which the records system was created.

SAFEGUARDS:

Access to and use of these records are limited to personnel whose official duties require such access. Personnel screening is employed to prevent unauthorized disclosure.

RETENTION AND DISPOSAL:

Records submitted by the individual, such as allotment authorization forms, home address forms, and tax withholding forms are retained until superseded by new forms or until the individual leaves the Department. Most of these records are then destroyed. Some of these records must be retained for an additional period, or forwarded to the new employing agency. Time and attendance records are retained for five years and are then destroyed. The automated payroll master record, established when the individual is first employed and continually updated throughout the period of his or her employment, is retained until the individual leaves the Department.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Pay Systems Division, P.O. Box 1823, Washington, D.C. 20013.

NOTIFICATION PROCEDURE:

An individual may contact the system manager. An individual also may contact, as appropriate, Payroll Liaison Representatives in Appendix 1 or Personnel Officers shown in HHS System 09900018, Applicants for Employment Record, Appendix 1. Provide name, social security number, timekeeper number and pay period about which inquiring.

RECORD ACCESS PROCEDURES:

Same as notification procedures. Requestors should also reasonably specify the record contents being sought. (These access procedures are in accordance with Department Regulations (45 CFR 5b.5(a)(2)) Federal Register, October 8, 1975, page 47410).

CONTESTING RECORD PROCEDURES:

Contact the official at the address specified under notification procedures above, and reasonably identify the record and specify the information to be contested, and state the corrective action sought and the reasons for the correction with supporting justification. (These procedures are in accordance with Department Regulations (45 CFR 5b.7) *Federal Register*, October 8, 1975, page 47411.).

RECORD SOURCE CATEGORIES:

Information in this system of records is (1) supplied directly by the individual, or (2) derived from information supplied by the individual, or (3) supplied by timekeepers and other Department officials.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

Appendix 1

Office of the Secretary

Payroll Liaison Officer, Room 4350 HHS North Bldg., 330 Independence Ave., SW., Washington, D.C. 20201

Health Care Financing Administration

Payroll Liaison Officer, HCFA, East Low Rise Building, P.O. Box 17255, Baltimore, MD 21203

Office of Human Development Services

Payroll Liaison Officer, Room 347 D, Hubert H. Humphrey Building, 200 Independence Ave., SW., Washington, DC 20201

Office of Child Support Enforcement

Payroll Liaison Officer, Room 1010 Parkway View Bldg., 6110 Executive Blvd, Rockville, MD 20852

Social Security Administration Headquarters

Payroll Liaison Officer, SSA Headquarters, Room L 1100 West Low Rise Bldg., 6401 Security Blvd., Baltimore, MD 21235

Payroll Liaison Officer, SSA, ORS, Universal Bldg., Room 894, 1875 Connecticut Ave., NW., Washington, D.C. 20009

Regional Offices

Region I, Payroll Liaison Officer, JFK Federal Bldg., Room 1808, Government Center, Boston, MA 02203

Region II, Payroll Liaison Officer, Personnel Support Branch, Room 38-130, 26 Federal Plaza, New York, NY 10007

Region III, Payroll Liaison Officer, P.O. Box 13716, Philadelphia, PA 19101

Region IV, Payroll Liaison Officer, 101 Marietta Tower, Suite 1601, Atlanta, GA 30323

Region V, Office of Personnel 21st Floor, Payroll Liaison Officer, 300 South Wacker Drive, Chicago, IL 60606

Region VI, Regional Personnel Office, Room 1005, 1200 Main Street, Dallas, TX 75202
Region VII, Payroll Liaison Officer, Regional Personnel Office, 601 E 12th Street, Kansas City, MO 64106
Region VIII, Payroll Liaison Officer, Federal Office Building, Room 1026, 19th and Stout Street, Denver, CO 80294
Region IX, Regional Personnel Office, Room 136A, 50 United Nations Plaza, San Francisco, CA 94102
Region X, Payroll Liaison Officer, Regional Personnel, Arcade Plaza Bldg., Mail Stop 607, 1321 Second Avenue, Seattle, WA 98101
Regional Personnel Branch Office, Payroll Liaison Officer, 24000 Avila Road, 6th Floor, Laguna Niguel, CA 92677
Regional Personnel Branch Office, Payroll Liaison Officer, 1301 Superior Avenue—Suite 240, Cleveland, OH 44114

Social Security Administration Program Centers

Mid Atlantic, Payroll Liaison Officer, Program Service Center, P.O. Box 8878, Philadelphia, PA 19122
Great Lakes, Payroll Liaison Officer, Program Service Center, 600 West Madison St., Chicago, IL 60606
Southeastern, Payroll Liaison Officer, Birmingham Program Service Center, P.O. Box 10304, Birmingham, AL 35202
North Eastern Payroll Liaison Officer, Program Service Center, 9605 Horace Harding Expressway, Flushing, NY 11368
Mid-American, Payroll Liaison Officer, Program Service Center, 601 East 12th Street, Kansas City, MO 64106
Western, Payroll Liaison Officer, Richmond Personnel Operations Center, Program Service Center, P.O. Box 2471, Richmond, CA 94802

Social Security Administration District Offices

New York, SSA, Payroll Liaison Officer, 26 Federal Plaza, Room 40-114, New York, NY 10007
Philadelphia,SSA, Payroll Liaison Officer, P.O. Box 12716, Philadelphia, PA 19101
Chicago, SSA, Payroll Liaison Officer, 300 South Wacker Drive, Chicago, IL 60606
Kansas City, SSA, Payroll Liaison Officer, 601 E 12th Street, Kansas City, MO 64106
San Francisco, Payroll Liaison Officer, Room 136A, 50 United Nations Plaza, San Francisco, CA 94102
Cleveland, SSA, Payroll Liaison Officer, 1301 Superior Avenue—Suite 240, Cleveland, OH 44114
SSA, Wilkes Barre Data Operations Center, Room 405, VA Bldg., 19 N. Main Street, Wilkes Barre, PA 18701
SSA Data Operations Center, Payroll Liaison Officer, P.O. Box 4429, Station A, Albuquerque, NM 87106
Boston, SSA, Payroll Liaison Officer, SSA, Room 1100, JFK Bldg., Government Center, Boston, MA 02203
Atlanta, SSA, Payroll Liaison Officer, 101 Marietta Tower, Suite 1801, Atlanta, GA 30301
Dallas, SSA, Payroll Liaison Officer, Room 1035, 1200 Main Street, Dallas, TX 75202
Denver, SSA, Payroll Liaison Officer, Federal Office Building, Room 1106, 19th and Stout Street, Denver, CO 80294
Seattle, SSA, Payroll Liaison Officer, Regional Personnel, Arcade Plaza Bldg., Mail Stop 607, 1321 Second Avenue, Seattle, WA 98101
SSA, Record Center, P.O. Box 28, Boyers, PA 16020
SSA Data Operations Center, Payroll Liaison Officer, 100 East Alvin Drive, Salinas, CA 93906
SSA, Office of Hearings and Appeals, Room 105, [illegible] Building, [illegible] Fairfax Drive, Arlington, VA 22203

Public Health Service

Center for Disease Control, Payroll Liaison Officer, Personnel Management Office, 1600 Clifton Road NE, Atlanta, GA 30333
National Inst. of Environmental Health Services Payroll Liaison Officer, P.O. Box 12233, Research Triangle Park, NC 27709
Food & Drug Administration, Payroll Liaison Officer, HFA 120 Parklawn Bldg., Room 11B, 5600 Fishers Lane, Rockville, MD 20857
Alcohol, Drug Abuse and Mental Health Administration, Payroll Liaison Officer, Room 13?? , Parklawn Bldg., 5600 Fishers Lane, Rockville, MD 20857
National Institute of Health, Payroll Liaison Officer, Bldg. 31, Room B1B 30, 9000 Rockville Pike, Bethesda, MD 20014
Health Resources and Services Admin & Office of Asst. Sec. for Health, Payroll Liaison Officer, Room 1648, Parklawn Bldg., 5600 Fishers Lane, Rockville, MD 20857
CDC, NIOSH, Payroll Liaison Officer, Financial Management Branch, Parklawn Bldg. 6A-10, 5600 Fishers Lane, Rockville, MD 20857

Indian Health Service

Payroll Liaison Officer, Indian Health Service Area Office, Room 215, Federal Building, Aberdeen, SD 57401
Payroll Liaison Officer, Albuquerque Indian Health Service, Federal Office Building and U.S. Courthouse, Room 4005, 500 Gold SW, Albuquerque, NM 87101
Payroll Liaison Officer, Alaska Area Native Health Service, Area Personnel and Training Branch, P.O. Box 7-741, Anchorage, AK 99501
Payroll Liaison Officer, Phoenix Area Indian Health Service, 3738 N. 16th Street, Suite A, Phoenix, AZ 85016
Payroll Liaison Officer, Oklahoma City Area Indian Health Service, 388 Old Post Office & Courthouse Bldg., Oklahoma City, OK 73102
Payroll Liaison Officer, Indian Health Service, 1220 SW. 3rd Avenue, Room 476, Portland, OR 97204
Payroll Liaison Officer, Indian Health Service Area Office, P.O. Box 2143, Billings, MT 59103
Payroll Liaison Officer, Navajo Area Indian Health Service, P.O. Box G, Attn: Financial Management Branch, Window Rock, AZ 86515
Payroll Liaison Officer, Indian Health Service, Data Processing Center, 2401 12th Street NW.—Room 3N, Albuquerque, NM 87102
Payroll Liaison Officer, Phoenix Indian Medical Center, 4212 N. 16th St., Phoenix, AZ 85016
Payroll Liaison Officer, Office of Research and Development, P.O. Box 11340, Tucson, AZ 85734
Payroll Liaison Officer, Gallup Indian Medical Center, P.O. Box 1337, Gallup NM

Public Health Service Hospitals

Payroll Liaison Officer, St Elizabeth's Hospital, Room 101 E. Building, 2700 Martin Luther King Ave., SE., Washington, D.C. 20032
Payroll Liaison Officer, USPHS Hospital, Carville, LA 70721

[FR Doc. [illegible] Filed 5-17-83; 8:45 am]
BILLING CODE [illegible]

Privacy Act of 1974; Proposed New Routine Use

AGENCY: Office of Personnel Management.

ACTION: Proposal for a new routine use to be added to an existing system of records.

SUMMARY: The purpose of this document is to propose a new routine use for the Office's General Personnel Records system (OPM/GOVT-1). This routine use, once in effect, will permit the disclosure of data from the Office's Central Personnel Data File (CPDF) to agencies and organizations that provide Federal assistance to employees of the Federal government. The disclosure of this information will be used for duly authorized matching programs.

COMMENT PERIOD: Any interested party may submit written comments regarding this proposal. To be considered, comments must be received on or before March 29, 1982.

ADDRESS: Address comments to: Assistant Director for Work Force Information, Office of Personnel Management (Room 5466), 1900 E Street, NW., Washington, D.C. 20415. Comments received will be available for public inspection at the above address from 9 a.m. to 4 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: John Sanet, Work Force Records Management Division, (202) 254-6792.

SUPPLEMENTARY INFORMATION: Recent reviews of various Federal assistance programs have indicated that some Federal employees may have improperly received government assistance, or have outstanding debts that are not being repaid to the Federal government. Specifically, the improper receipt of government assistance in the U.S. Department of Agriculture's Food Stamp and the Veterans Administration's Compensation and Pension programs generally based upon fraudulently prepared applications which fail to disclose Federal employment have been identified. In addition, delinquent repayment of debts and defaulted loans by Federal employees have been identified in Health and Human Service's student loan and the Veterans Administration's educational assistance programs. The President's Council on Integrity and Efficiency (PCIE) believes that it is prudent to identify Federal employees, on a government-wide basis, who have improperly received benefits or have delinquent debts.

The objectives of this part of the PCIE project are twofold: (1) To identify Federal employees or retirees who may be erroneously or fraudulently receiving government payments, and (2) to identify Federal employees or retirees who are indebted to the government and then to initiate appropriate collection action.

The most efficient way of comparing individuals who are recipients of various Federal assistance programs with those who are active Federal civilian employees is for OPM to provide an extract of its Central Personnel Data File (CPDF) tape with various relevant data elements to the agencies conducting these various assistance programs. (These agencies and programs are cited below and the data provided by OPM will be strictly limited to that listed).

The disclosure of individual data from the CPDF to these agencies will be for the purpose of conducting matching programs. The CPDF is part of the OPM/GOVT-1 system of records. The matches will be conducted in accordance with the Office of Management and Budget's Supplemental Guidance for Matching Programs (44 FR 23138; April 18, 1979).

During OPM's participation in the formulation of this matching project, it was the Office's position that information could be disclosed from the CPDF only if the various recipient agencies agreed to strictly adhere to OMB's Matching Guidelines. The agencies cited below will be required to submit written requests for the Office's information, including written assurance by the agency Inspector General that the privacy concerns expressed in the Matching Guidelines will be followed.

Information on individuals that may be disclosed to the various matching agencies through this routine use includes: Name, social security number, date of birth, sex, annualized salary rate, service computation date, separation date, handicap, veterans preference, retirement status, occupational series, position occupied, work schedule, agency identifier, agency subelement identifier, geographic location, special program identifier, and submitting office number. The Office retains the authority under the proposed routine use to withhold data from a requesting agency if it is believed that the particular data requested are not germane to the particular benefit program.

Upon receipt of this information or a portion thereof, and compliance with the OMB Guidelines on Matching Programs, the agencies will match it against their various files involving benefit recipients. For each match it is anticipated that the agencies will conduct a more thorough review of the recipient's status as to eligibility for assistance and the status of any debt that is owed to the Government.

Under Office regulations (5 CFR 294.702), the disclosure of the name, agency, salary, and duty station location (including agency identifier, agency subelement identifier, and submitting office number) is permitted without the data subject's prior approval. Thus, the routine use is necessary to permit the disclosure of the other data cited in the proposed routine use. Though these other data are not considered to be public information, anticipated benefits to the public justify disclosure of this information for matching purposes with these agencies under safeguards established by those agencies jointly with the Office to protect against unauthorized disclosure.

Disclosure under the proposed routine use will permit the agencies to assure greater integrity of their various programs and is compatible with Federal personnel management responsibility for oversight of Federal employee's conduct, particularly with the requirment that employees conduct themselves in a proper manner, not obtain financial benefits in a fradulent manner, and pay their just obligations.

The Office fully recognizes that in this particular project authorized by this particular routine use, only the records of Federal employees are being examined and has taken certain steps to protect the privacy of those individuals while furthering the goals of eliminating waste, fraud, and abuse in the numerous recipient programs administered by the Federal government. Care has been taken to determine the best approach to take to permit the Office's participation and also to comply with the intent of the Privacy Act. Analysis of these concerns was accomomplished not only by the Office staff, but by various agencies of the Federal community. The result of this study was a clear determination that a matching program of this magnitude could be conducted without violating the Privacy Act if the conditions described in OMB's Matching Guidelines were followed.

The following agency programs which may be included in the PCIE computer matching project "Federal Employees Receiving Government Assistance," are listed below with the public law authorizing each program cited where appropriate.

I. Department of Agriculture

Food Stamp Program and Commodities in Lieu of Food Stamps. Pub. L. 95-113, The Food Stamp Act of 1977, as amended.

National School Lunch Program.
School Breakfast Program.
Special Milk Program.
Child Care Food Program.
Special Supplemental Food Programs.
Summer Food Service Programs. Pub. L. 79-396, National School Lunch Act of 1946, as amended; Pub. L. 89-642, Child Nutrition Act of 1966 as amended; and Pub. L. 95-313 (7 U.S.C. 612), Agriculture and Consumer Protection Act of 1973, as amended.
Elderly Feeding Program. Pub. L. 92-258 (42 U.S.C. 3030), Older Americans Act of 1965 and 1978, as amended; and Pub. L. 97-35, The 1981 Omnibus Reconciliation Act.
Rural Housing Support Programs.
Very Low-Income Housing Repair Programs.
Rural Low-Income Multi-Family Housing Program.
Rural Moderate-Income Multi-Family Housing Program.
Rural Moderate-Income Single Family Housing Loan Program.
Above Moderate-Income Single Family Housing Program.
Rural Low-Income Single Family Housing Program.
Rural Rental Assistance and Home Ownership Assistance Programs.
Farm Labor Housing Program. 83 Stat. 432, Title V of the Housing Act of 1949, as ameded.
Farm Real Estate Loan Program.
Emergency Loan Programs.
Business and Industrial Loan Program. Pub. L. 87-128, Consolidated Farm and Rural Development Act, as amended; and Pub. L. 95-334, Emergency Agricultural Credit Adjustment Act of 1978, as amended.

II. Department of Education

The following Department of Education programs are authorized by Pub. L. 96-374, the Higher Education Act, Title IV. The pertinent parts of Title IV, applying to specific programs, are indicated for each.

Basic Educational Opportunity Grants (Pell Grants).
Supplemental Educational Opportunity Grants. Title IV (Part A).
Guaranteed Student Loan Program. Title IV (Part B).
National Direct Student Loan Program. Title IV (Part D).

III. Department of Health and Human Services

Aid to Families with Dependent Children (AFDC): Pub. L. 74-271 (42 U.S.C. Subchapter IV), Title IV-A of the Social Security Act of 1935, as amended by Pub. L.'s. 92-603, 93-66, 93-233 and 95-216.
Black Lung Benefit Programs: Pub. L. 91-173, Federal Coal Mine Health and Safety Act of 1969, Title IV and Pub. L. 92-303, Black Lung Benefit Act of 1972, as amended by Pub. L. 95-239.
Health Professionals Educational Assistance Act of 1968: Pub. L. 92-157 as amended by Pub. L. 94-484.

IV. Department of Labor

Federal Employees Compensation Program. Pub. L. 93-416, Federal Employees Compensation Act (FECA).
Longshoremen's and Harbor Workers' Compensation Program. Pub. L. 92-576, Longshoremen's and Harbor Workers' Compensation Act Amendment of 1972.
Black Lung Benefits. Pub. L. 95-239, Black Lung Benefit Reform Act of 1977.

V. Department of Transportation

Title V Employee Protection Program. Pub. L. 93-236, Regional Railroad Reorganization Act of 1973, as amended by Pub. L. 96-448, Staggers Rail Act of 1980.

VI. Veterans Administration

The following VA programs are authorized by Title 38 U.S.C., Chapter 3, Section 210(c)(1). Additional chapters of Title 38, applying to specific programs, are indicated for each.

Patient Medical Records—VA (24 VA 136). Chapter 17.
Veterans, Dependents, and Beneficiaries Compensation and Pension Records—VA (49 VA 21). Chapters 11, 13, 15, and 23.
Veterans, Dependents, Beneficiaries, and Armed Forces Personnel Education and Rehabilitation Records—VA (50 VA 22). Chapters 31, 32, 34, 35, and 36.
Veterans and Beneficiaires Identification and Records Locator System—VA (38 VA 28).
TARGET System—Compensation, Pension, Education, and Rehabilitation Records—VA (58 VA 21/22). Chapters 11, 13, 15, 17, 23, 31, 32, 34, 35, 36.
Loan Guaranty Home, Condominium, Mobile Home Loan Applicant Records and Paraplegic Grant Application Records—VA 55 (VA 26) Chapters 21 and 27

A match between the CPDF and the agencies' programs is not an indication that any illegality has occurred; the match will alert the agencies, however, that further study is warranted to see if there is any impropriety.

U.S. Office of Personnel Management.
Donald J. Devine,
Director.

PROPOSED ROUTINE USE:

The following routine use will be added to the Office of Personnel Management's government-wide system of records (OPM/GOVT-1). The current notice of this system is published at 45 FR 78415 et seq. (November 25, 1980).

OPM/GOVT-1

SYSTEM NAME:

General Personnel Records.

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

* * * * *

gg. To disclose information contained in the Central Personnel Data File including the name, social security number, date of birth, sex, annualized salary rate, service computation date of basic active service date, separation or retirement date, reportable handicap, veteran's preference, retirement status, occupational series, position occupied, work schedule (full time, part time, or intermittent), agency identifier, geographic location (duty station location), standard metropolitan service area, special program identifier, submitting office number of all Federal employees to agencies participating in the "Federal Employee Receiving Government Assistance" Matching Project conducted by the President's Council on Integrity and Efficiency to help eliminate fraud and abuse in the benefit program administred by agencies within the Federal government and to collect debts and overpayment owed to the Federal government.

* * * * *

[FR Doc. [illegible] Filed [illegible] 8:45 am]

BILLING CODE [illegible]

Attachment F

Matching Agency (VA) Routine Use Notice

F1 Request for Publication of Notice

F2 Notice as Published in the Federal Register

COPY

Veterans Administration

Memorandum

To: Chief Benefits Director (20)

Date: December 23, 1981

Subj: President's Council on Integrity and Efficiency Project: "Federal Employees Receiving Government Assistance"

1. As part of the VA's participation in this project, my office plans to conduct a series of computer matches. The matches will compare Federal military and civilian personnel files with certain VA program files for the purpose of identifying and locating individuals who either have overdue indebtedness to the VA or have received VA benefits to which they are not entitled. The goal of these matches is to determine names and current locations (office and/or home) of individuals who meet the selection criteria for each match. This will provide information needed to initiate appropriate collection actions and/or follow-up on previously initiated actions using more current addresses.

2. We would like you to make the necessary arrangements with the Office of Data Management and Telecommunications for us to use the automated systems of records identified in paragraph 3. In addition, please establish a point of contact within your department to facilitate coordination of these matches. Inform us of his/her name and telephone number by December 31, 1981.

3. Personnel records to be used for these matches include those of active and retired civilian and military personnel maintained by OPM, DOD, TVA, and US Coast Guard, FBI, CIA, and the National Security Agency. VA program files, maintained by your department, to be matched against those personnel files are:

a. Veterans, Dependents, and Beneficiaries Compensation and Pension Records - VA (49 VA 21).

b. Veterans, Dependents, Beneficiaries, and Armed Forces Personnel Education and Rehabilitation Records - VA (50 VA 22).

c. TARGET System - Compensation, Pension, Education, and Rehabilitation Records - VA (58 VA 21/22).

d. Loan Guaranty Home, Condominium, Mobile Home Loan Applicant Records and Paraplegic Grant Application Records - VA (55 VA 26).

e. Veterans, Beneficiaries, and Attorneys U.S. Government Insurance Award Records - VA (46 VA 00).

4. In order to meet the requirements of the Privacy Act of 1974 and the OMB Guidelines for Computer Matching, this office will publish a Matching Report, after coordination with your staff. This report will go to the Director, OMB; the President of the Senate; the Speaker of the House; and the Federal Register (for publication). An additional requirement is to amend the previously pub-

COPY

lished systems notice for each VA system of records to be matched (see MPI, Part II, Chapter 21, Appendix B). The records produced by each match will be a subset of the major system of records used in the match. The amendments will permit release of the resultant data to program managers and others for collection actions. Suggested wording for the amendments is shown in Enclosure 1.

5. The necessary amendments should be published in the Federal Register as soon as possible so that we may expeditiously pursue the matches. Would you advise us by January 15, 1982, of the final text of the amendments and the date(s) of publication. If you have any questions or require assistance concerning this matter, please contact Mr. James Durnil on extension 2901 or Ms. Yvonne Carter on extension 2403/8.

"signed"

BOBBY B. OAKLEY
Assistant Inspector General
for Auditing (52)

Enclosure

ENCLOSURE 1

SUGGESTED AMENDMENTS TO SYSTEM NOTICES

(DM&S) For System 24 VA 136.
(DVB) For Systems 38VA28, 46VA00, 49VA21, 50VA22,
55VA26, and 58VA 21/22.

Under paragraph "Categories of records", add:

> Some information maintained in this system of records such as Federal employment status and place of employment is associated with and may be obtained from computer matching programs involving employment records of this and other Federal agencies, both civilian and military.

Under paragraph "Routine uses ....", add:

> Any information from this system of records, including personal information obtained from other Federal agencies through computer matching programs, may be disclosed to Federal, state, and local governmental agencies, credit and debt collection activities, and law enforcement agencies for the purposes of: (a) assisting the VA in collection of benefit overpayments, overdue indebtedness, and/or costs of services provided individuals not entitled to such services, and (b) initiating legal actions for prosecuting individuals who willfully or fraudulently obtain benefits without entitlement.

VETERANS ADMINISTRATION

Privacy Act of 1974; Amendment of Systems Notice; Revised Routine Use Statements

Notice is hereby given that the VA (Veterans Administration) is considering adding a new routine use statement and revising current routine use number 11 for the system of VA records entitled "Compensation, Pension, Education and Rehabilitation Records—VA" (58VA21/22/28) as set forth on page 372 of the Federal Register of January 5, 1982. As part of the VA's participation in the President's Council of Integrity and Efficiency Project entitled "Federal Employees Receiving Government Assistance," the VA Office of Inspector General, in coordination with other Federal agencies, plans to conduct a series of computer matches. The matches will compare various Federal military and civilian personnel records with certain VA program records for the purpose of identifying and locating Federal employees who currently are indebted to the VA or have received VA benefits to which they are not entitled. The goal of the matches is to reduce the amount of outstanding debt owed by individuals to the VA as a result of an individual's participation in a VA benefits program. In order to utilize information generated by the match to initiate appropriate collection actions and/or follow-up on previously initiated actions, current routine use statement number 11 must be revised and a new routine use added. The routine uses will enable the disclosure of identifying and debt information to any third party, including consumer reporting agencies, in order to facilitate and expedite the collection process. Further, the new proposed routine use No. 42 permits the disclosure of information in order for the VA to initiate legal actions for prosecuting individuals who willfully or fraudulently obtain title 38 benefits without entitlement. The VA has determined that release of information for these purposes is necessary and a proper use of information in this system of records and that specific routine uses for transfer of this information are appropriate.

Interested persons are invited to submit written comments, suggestions, or objections regarding the proposed systems of records to the Administrator of Veterans Affairs (271A), Veterans Administration, 810 Vermont Avenue, NW., Washington, D.C. 20420. All relevant material received before May 16, 1982 will be considered. All written comments received will be available for public inspection at the above address only between the hours of 8 a.m. and 4:30 p.m. Monday through Friday (except holidays) until May 24, 1982. Any person visiting Central Office for the purpose of inspecting any such comments will be received by the Central Office Veterans Services Unit in room 132. Visitors to any VA field station will be informed that the records are available only in Central Office and furnished the above address and room number.

If no public comment is received during the 30-day review period allowed for public comment or unless otherwise published in the *Federal Register* by the Veterans Administration, the new and revised routine use statements included herein are effective May 5, 1982.

Approved: May 5, 1982.

Robert P. Nimmo,

Administrator.

Notice of Systems Records

In the system identified as 58VA21/22/28, "Compensation, Pension, Education and Rehabilitation Records-VA," appearing at 47 FR 372, the following changes are made:

SYSTEM NAME:

Compensation, Pension, Education and Rehabilitation Records-VA.

* * * * *

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

* * * * *

11. The name and address of a veteran, other information as is reasonably necessary to identify such veteran, including personal information obtained from other Federal agencies through computer matching programs, and any information concerning the veteran's indebtedness to the United States by virtue of the person's participation in a benefits program administered by the VA may be disclosed to a consumer reporting agency for purposes of assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 3301(g)(4) have been met.

* * * * *

42. Any information concerning the veteran's indebtedness to the United States by virtue of a person's participation in a benefits program administered by the VA, including personal information obtained from other Federal agencies through computer matching programs, may be disclosed to any third party, except consumer reporting agencies, in connection with any proceeding for the collection of any amount owed to the United States. Purposes of these disclosures may be to (a) assist the VA in collection of title 38 benefit overpayments, overdue indebtedness, and/or costs of services provided individuals not entitled to such services, and (b) initiate legal actions for prosecuting individuals who willfully or fraudulently obtain title 38 benefits without entitlement. This disclosure is consistent with 38 U.S.C. 3301(b)(6).

[FR Doc. 82-[illegible] Filed 4-13-82; 8:45 am]

BILLING CODE 8320-01-M

Attachment G

VA Matching Report Submissions

G1 Submission for Federal Register Publication

G2 Submission to OMB and Congress

VETERANS ADMINISTRATION

Computer Matching Program

Federal Personnel Indebted to the Veterans Administration

AGENCY: Veterans Administration

ACTION: Notice

SUMMARY: Notice is hereby given that the VA OIG (Veterans Administration Office of Inspector General), in coordination with other Federal agencies, is conducting a series of computer matches as part of the VA's participation in the President's Council on Integrity and Efficiency Project entitled "Federal Employees Receiving Government Assistance." The matches will compare various Federal military and civilian personnel records with certain VA program records for the purpose of identifying and locating Federal personnel who currently are indebted to the VA or have received VA benefits to which they are not entitled. The goals of the matches are to reduce the amount of outstanding debt owed by individuals to the VA, to identify and eliminate the methods by which individuals obtain benefits without entitlement, and to recoup the dollar-value of received benefits from individuals who were not entitled to the benefits. Administrative, personnel, and civil actions, as appropriate, will be used by the VA during the collection process which will follow the matches. For the information of all concerned, the text of the VA matching program report, describing these computer matches, follows. In accordance with the OMB Matching Guidelines, dated May 11, 1982, copies of this report have been sent to OMB and both Houses of Congress.

FOR FURTHER INFORMATION CONTACT: Jim Durnil (202) 389-2901

DATED: August 25, 1982

By direction of the Administrator:

Everett Alvarez Jr.
EVERETT ALVAREZ, JR.
Deputy Administrator

Certified to be a true copy
of the original.
Celia Fasone
Information & Regulations
Staff (004A1)

VETERANS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
Computer Matching Program

FEDERAL PERSONNEL INDEBTED TO THE VETERANS ADMINISTRATION

Authority for and Purpose of the Program:

The OIG (Office of Inspector General), pursuant to the authority granted by the Inspector General Act of 1978 (Public Law 95-452), has initiated a computer matching program. This program is designed to identify Federal personnel who have defaulted on VA loans or who have been provided VA benefits erroneously and from whom VA has been unable to collect. For purposes of this matching program, the term "Federal personnel" includes Federal civilian employees and retirees; U.S. Armed Forces active duty personnel, retirees, and reservists; and survivors/beneficiaries of individuals in any of these categories.

Description of the Matching Program:

This matching program will involve computer matches of Federal personnel data files from OPM (Office of Personnel Management), DOD (Department of Defense), TVA (Tennessee Valley Authority), and USCG (U.S. Coast Guard) with five VA program files described below. The VA program files are from two major program areas: Veterans Benefits Programs managed by the DVB (Department of Veterans Benefits) and Medical Service Programs managed by the DM&S (Department of Medicine and Surgery).

Files to be used in this matching program are:

a. Veterans Administration:

(1) Patient Medical Records - VA (24 VA 136), 42 F.R. 49739.

(2) Compensation, Pension, Education and Rehabilitation Records - VA (58 VA 21/22/28), 47 F.R. 372.

(3) Loan Guaranty Home, Condominium, Mobile Home Loan Applicant Records and Paraplegic Grant Applications Records - VA (55 VA 26), 42 F.R. 49758.

(4) Veterans, Beneficiaries and Attorneys U.S. Government Insurance Award Records - VA (46 VA 00), 47 F.R. 29432.

(5) Veterans and Armed Forces Personnel U.S. Government In-Force Life Insurance Records - VA (36 VA 00), 47 F.R. 29432.

(6) Veterans and Beneficiaries Identification and Records Location Subsystem - VA (38 VA 23), 47 F.R. 368.

b. Office of Personnel Management:

(1) General Personnel Records System (OPM/GOVT-1), specifically the Central Personnel Data File (CPDF) within this system of records, 45 F.R. 78415 et seq.

(2) Civil Service Retirement and Insurance Records System (OPM/Central-1), specifically the Civil Service Retirement and Insurance File within this system of records, 45 F.R. 78415 et seq.

c. Department of Defense (Defense Logistics Agency):

Defense Manpower Data Center Data Base (S322.10 DLA-LZ), 47 F.R. 2544.

d. Department of Transportation (U.S. Coast Guard):

(1) Active Duty Military Payroll System (DOT/CG 525), 46 F.R. 59752.

(2) Personnel Management Information System (DOT/CG 624), 46 F.R. 59766.

e. Tennessee Valley Authority:

(1) Personnel Files (TVA-2), 46 F.R. 62993.

(2) Payroll Records (TVA-11), 46 F.R. 62993.

(3) Retirement System Records (TVA-26), 46 F.R. 62993.

Objectives to be Met by the Matching Program:

The objectives of this matching program are to detect and identify Federal employees, retirees, or their survivors who have defaulted on VA loans or who have been provided VA benefits in error, and to provide sufficient locator information to permit initiation of collection or recoupment actions. While this program has been established as a one-time matching project, analysis of the results may support changing one or more of the individual matches to recurring projects.

Procedures of Matching Program:

Step 1. Acquisition of Data Files. The four source agencies will provide the VA OIG computer tapes containing personal information on Federal personnel. DVB and DM&S will make available to the OIG copies of automated program files containing information about persons on the compensation, pension, education, accounts receivable, insurance award, guaranteed/insured loan, and patient treatment systems. All files will be safeguarded in accordance with the National Bureau of Standards' Federal Information Processing Standards 41 and 31. The information provided to the OIG will be acquired, controlled, and used in compliance with the Privacy Act of 1974 (5 U.S.C. § 552a), 38 U.S.C. §§ 3301 and 4132, implementing VA regulations, and the OMB Matching Guidelines, dated May 11, 1982.

Step 2. Computer Processing. The OIG Office of Audit will conduct the computer matching of the files. Results of the matches will be turned over to DVB or DM&S, as appropriate, for followup action.

Step 3. Routine Collection. DVB and DM&S will review the products of the match to determine the individuals for whom collection procedures should be initiated or reopened. VA will attempt to contact those individuals to try to resolve the accounts. VA will work with those responding who deny or dispute the liability.

Step 4. Federal Employee Assistance. VA will take the following actions concerning Federal employees who fail to respond to direct contact attempts:

(a) A letter will be sent to the debtor at his or her Federal employing agency requesting that the person immediately contact the VA. PERSONAL/PRIVATE-TO BE OPENED BY ADDRESSEE ONLY will be stamped in a prominent location on the envelope. The envelope will also contain a request that a forwarding address be furnished if the letter is undeliverable as addressed.

(b) Each Federally employed debtor will have 60 days to respond. If the debtor is still nonresponsive, the employing agency will be asked to contact the employee about his or her indebtedness. With the concurrence of the VA General Counsel, a listing of those debtors for whom personal contact is being requested will be provided to the responsible administrative office for the employing agency.

Step 5. Litigation. The merits of each claim remaining unresolved will be reviewed and, if appropriate, the claim will be referred for followup action by a U.S. Attorney or VA District Counsel. Where there are reasonable grounds to believe there has been a violation of criminal law, the matter will be referred to the appropriate authorities for investigation and consideration of criminal prosecution.

Step 6. Records Maintained by DVB and DM&S. Any manual records resulting from the match will be maintained by DVB and DM&S. As claims are settled or repaid, the various files will be updated to reflect these changes.

Date of Matching Program:

In accordance with the OMB Matching Guidelines, the computer matches were initiated after the publication of the routine use notices for all systems of records involved in the matching program. The match programs and referral of cases to DVB and DM&S should be completed during Fiscal Year 1982. The period of time which will be required by DVB and DM&S for completion of collection actions cannot be determined.

Disclosure of Records:

a. VA Systems of Records Extracts to OIG. The transfer of extracts from the five VA Systems of Records to the OIG for performing the matches is an intra-agency "need-to-know" disclosure permitted under 5 U.S.C. 552 a(b)(1) and is consistent with the statutory language creating the OIG which is found in Section 6 (a)(1) of Public Law 95-452.

b. Source Agency Records to OIG. The transfer of extracts from the personnel files of the four source agencies to the OIG for performance of the matches will be carried out pursuant to the agencies' publications of routine use notices in the *Federal Register*. On completion of the match program, source agency files will be returned to their originators or electronically erased to prevent further access.

c. Transfer of Match Products from OIG to DVB and DM&S. The transfer of the products of the match (e.g., name, SSN, date of birth of the potential debtor) from the VA OIG to DVB and DM&S is an intra-agency, "need-to-know" disclosure permitted under 5 U.S.C. 552 a(b)(1). Valid match information will become part of the appropriate VA system of records. Invalid match information will be erased or destroyed.

d. VA Request for Personnel Contact by Federal Employing Agencies. The transfer of information between VA and Federal employing agencies to permit personal contact of Federal employees is pursuant to the routine uses published in the *Federal Register* for the five VA systems of records.

e. Referral of Claims for Litigation. As appropriate, cases will be referred to U.S. Attorneys or VA District Counsels for the respective agency systems of records.

Efforts Taken to Protect Against Unauthorized Access to or Disclosure of Personal Records:

a. The procedures set forth for the implementation of the proposed matching program incorporate (1) strong provisions to assure that the information disclosed is adequately safeguarded and that unwarranted disclosures do not occur, and (2) existing statutes and regulations regarding indebtedness of Federal employees.

b. Federal personnel identified as potentially receiving benefits without entitlement will have their eligibility for and receipt of VA benefits verified by DVB or DM&S, and those determined to be eligible for the benefits they are receiving will have no information disclosed from their records. Federal personnel identified as being in debt to the VA but in satisfactory adherence to repayment plans will have no information disclosed from their records. VA regulations and 38 U.S.C. 3102 and 4005a provide for waiver and subsequent appeal by any individual who feels that an appeal is warranted. Every effort will be made to ensure that each individual's personal and privacy rights are protected.

Office of Inspector General
Washington, D.C. 20420

Veterans Administration

COPY

September 9, 1982

In Reply Refer To: (52)

Honorable Thomas P. O'Neill, Jr.
Speaker of the House of
Representatives
Washington, DC 20510

Dear Mr. Speaker:

Enclosed is a copy of the Veterans Administration's matching program report which has been released for publication in the Federal Register. We have also sent copies to the President of the Senate and the Office of Management and Budget. These matches are being conducted under the auspices of the President's Council on Integrity and Efficiency.

Your staff may address inquiries and comments concerning the matching program to Mr. James B. Durnil, Acting Deputy Assistant Inspector General for Headquarters Audits. Correspondence for Mr. Durnil should be sent to Veterans Administration (52); 810 Vermont Avenue, NW; Washington, DC 20420. Mr. Durnil may be reached by telephone at 389-2901.

Sincerely,

"signed"

FRANK S. SATO
Inspector General

Enclosure

VETERANS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
Computer Matching Program

FEDERAL PERSONNEL INDEBTED TO THE VETERANS ADMINISTRATION

Authority for and Purpose of the Program:

The OIG (Office of Inspector General), pursuant to the authority granted by the Inspector General Act of 1978 (Public Law 95-452), has initiated a computer matching program. This program is designed to identify Federal personnel who have defaulted on VA loans or who have been provided VA benefits erroneously and from whom VA has been unable to collect. For purposes of this matching program, the term "Federal personnel" includes Federal civilian employees and retirees; U.S. Armed Forces active duty personnel, retirees, and reservists; and survivors/beneficiaries of individuals in any of these categories.

Description of the Matching Program:

This matching program will involve computer matches of Federal personnel data files from OPM (Office of Personnel Management), DOD (Department of Defense), TVA (Tennessee Valley Authority), and USCG (U.S. Coast Guard) with five VA program files described below. The VA program files are from two major program areas: Veterans Benefits Programs managed by the DVB (Department of Veterans Benefits) and Medical Service Programs managed by the DM&S (Department of Medicine and Surgery).

Files to be used in this matching program are:

a. Veterans Administration:

(1) Patient Medical Records - VA (24 VA 136), 42 F.R. 49739.

(2) Compensation, Pension, Education and Rehabilitation Records - VA (58 VA 21/22/28), 47 F.R. 372.

(3) Loan Guaranty Home, Condominium, Mobile Home Loan Applicant Records and Paraplegic Grant Applications Records - VA (55 VA 26), 42 F.R. 49758.

(4) Veterans Beneficiaries and Attorneys U.S. Government Insurance Award Records - VA (46 VA 00), 47 F.R. 29432.

(5) Veterans and Armed Forces Personnel U.S. Government In-Force Life Insurance Records - VA (36 VA 00), 47 F.R. 29432.

(6) Veterans and Beneficiaries Identification and Records Location Subsystem - VA (38 VA 23), 47 F.R. 368.

b. Office of Personnel Management:

(1) General Personnel Records System (OPM/GOVT-1), specifically the Central Personnel Data File (CPDF) within this system of records, 45 F.R. 78415 et seq.

(2) Civil Service Retirement and Insurance Records System (OPM/Central-1), specifically the Civil Service Retirement and Insurance File within this system of records, 45 F.R. 78415 et seq.

c. Department of Defense (Defense Logistics Agency):

Defense Manpower Data Center Data Base (S322.10 DLA-LZ), 47 F.R. 2544.

d. Department of Transportation (U.S. Coast Guard):

(1) Active Duty Military Payroll System (DOT/CG 525), 45 F.R. 59752.

(2) Personnel Management Information System (DOT/CG 624), 46 F.R. 59766.

e. Tennessee Valley Authority:

(1) Personnel Files (TVA-2), 46 F.R. 62993.

(2) Payroll Records (TVA-11), 46 F.R. 62993.

(3) Retirement System Records (TVA-26), 46 F.R. 62993.

Objectives to be Met by the Matching Program:

The objectives of this matching program are to detect and identify Federal employees, retirees, or their survivors who have defaulted on VA loans or who have been provided VA benefits in error, and to provide sufficient locator information to permit initiation of collection or recoupment actions. While this program has been established as a one-time matching project, analysis of the results may support changing one or more of the individual matches to recurring projects.

Procedures of Matching Program:

Step 1. Acquisition of Data Files. The four source agencies will provide the VA OIG computer tapes containing personal information on Federal personnel. DVB and DM&S will make available to the OIG copies of automated program files containing information about persons on the compensation, pension, education, accounts receivable, insurance award, guaranteed/insured loan, and patient treatment systems. All files will be safeguarded in accordance with the National Bureau of Standards' Federal Information Processing Standards 41 and 31. The information provided to the

OIG will be acquired, controlled, and used in compliance with the Privacy Act of 1974 (5 U.S.C. § 552a), 38 U.S.C. §§ 3301 and 4132, implementing VA regulations, and the OMB Matching Guidelines, dated May 11, 1982.

Step 2. Computer Processing. The OIG Office of Audit will conduct the computer matching of the files. Results of the matches will be turned over to DVB or DM&S, as appropriate, for followup action.

Step 3. Routine Collection. DVB and DM&S will review the products of the match to determine the individuals for whom collection procedures should be initiated or reopened. VA will attempt to contact those individuals to try to resolve the accounts. VA will work with those responding who deny or dispute the liability.

Step 4. Federal Employee Assistance. VA will take the following actions concerning Federal employees who fail to respond to direct contact attempts:

(a) A letter will be sent to the debtor at his or her Federal employing agency requesting that the person immediately contact the VA. PERSONAL/PRIVATE-TO BE OPENED BY ADDRESSEE ONLY will be stamped in a prominent location on the envelope. The envelope will also contain a request that a forwarding address be furnished if the letter is undeliverable as addressed.

(b) Each Federally employed debtor will have 60 days to respond. If the debtor is still nonresponsive, the employing agency will be asked to contact the employee about his or her indebtedness. With the concurrence of the VA General Counsel, a listing of those debtors for whom personal contact is being requested will be provided to the responsible administrative office for the employing agency.

Step 5. Litigation. The merits of each claim remaining unresolved will be reviewed and, if appropriate, the claim will be referred for followup action by a U.S. Attorney or VA District Counsel. Where there are reasonable grounds to believe there has been a violation of criminal law, the matter will be referred to the appropriate authorities for investigation and consideration of criminal prosecution.

Step 6. Records Maintained by DVB and DM&S. Any manual records resulting from the match will be maintained by DVB and DM&S. As claims are settled or repaid, the various files will be updated to reflect these changes.

Date of Matching Program:

In accordance with the OMB Matching Guidelines, the computer matches were initiated after the publication of the routine use notices for all systems of records involved in the matching program. The match programs and referral of cases to DVB and DM&S should be completed during Fiscal Year 1982. The period of time which will be required by DVB and DM&S for completion of collection actions cannot be determined.

Disclosure of Records:

a. VA Systems of Records Extracts to OIG. The transfer of extracts from the five VA Systems of Records to the OIG for performing the matches is an intra-agency "need-to-know" disclosure permitted under 5 U.S.C. 552 a(b)(1) and is consistent with the statutory language creating the OIG which is found in Section 6 (a)(1) of Public Law 95-452.

b. Source Agency Records to OIG. The transfer of extracts from the personnel files of the four source agencies to the OIG for performance of the matches will be carried out pursuant to the agencies' publications of routine use notices in the Federal Register. On completion of the match program, source agency files will be returned to their originators or electronically erased to prevent further access.

c. Transfer of Match Products from OIG to DVB and DM&S. The transfer of the products of the match (e.g., name, SSN, date of birth of the potential debtor) from the VA OIG to DVB and DM&S is an intra-agency, "need-to-know" disclosure permitted under 5 U.S.C. 552 a(b)(1). Valid match information will become part of the appropriate VA system of records. Invalid match information will be erased or destroyed.

d. VA Request for Personnel Contact by Federal Employing Agencies. The transfer of information between VA and Federal employing agencies to permit personal contact of Federal employees is pursuant to the routine uses published in the Federal Register for the five VA systems of records.

e. Referral of Claims for Litigation. As appropriate, cases will be referred to U. S. Attorneys or VA District Counsels for collection actions pursuant to published routine use notices for the respective agency systems of records.

Efforts Taken to Protect Against Unauthorized Access to or Disclosure of Personal Records:

a. The procedures set forth for the implementation of the proposed matching program incorporate (1) strong provisions to assure that the information disclosed is adequately safeguarded and that unwarranted disclosures do not occur, and (2) existing statutes and regulations regarding indebtedness of Federal employees.

b. Federal personnel identified as potentially receiving benefits without entitlement will have their eligibility for and receipt of VA benefits verified by DVB or DM&S, and those determined to be eligible for the benefits they are receiving will have no information disclosed from their records. Federal personnel identified as being in debt to the VA but in satisfactory adherence to repayment plans will have no information disclosed from their records. VA regulations and 38 U.S.C. 3102 and 4005a provide for waiver and subsequent appeal by any individual who feels that an appeal is warranted. Every effort will be made to ensure that each individual's personal and privacy rights are protected.

Attachment H

Matching Reports to the Federal Register

H1 HHS Office of Inspector General

H2 HHS-Social Security Administration

H3 VA-Office of Inspector General

Office of the Secretary

Privacy Act of 1974; Matching Program—Federal Personnel/AFDC and Black Lung Benefit Records

AGENCY: Health and Human Services Department.

ACTION: Notification of a Matching Program—Federal Personnel/AFDC and Black Lung Benefit Records.

SUMMARY: The Department of Health and Human Services is providing notice that the Office of Inspector General intends to conduct matches of federal personnel records of the Office of Personnel Management, the Department of Defense, the United States Coast Guard, and the Tennessee Valley Authority with State Aid to Families with Dependent Children (AFDC) records and Social Security Black Lung Payment information. A matching report is set forth below.

DATES: These matches will begin in September and October 1982.

ADDRESS: Send any comments to Office of Public Affairs, Office of Inspector General, Department of Health and Human Services, Room 5267, HHS North Building, 330 Independence Avenue, SW., Washington, D.C. 20201.

FOR FURTHER INFORMATION CONTACT: Richard McGowan, Public Affairs Officer, Office of Inspector General, Department of Health and Human Services, Room 5267 HHS North Building, 330 Independence Avenue, SW., Washington, D.C. 20201 or call (202) 472-3142.

SUPPLEMENTARY INFORMATION: The Office of Inspector General under the auspices of the President's Council on Integrity and Efficiency has initiated a major project to reduce fraud and abuse by federal employees, retirees, or survivors who are improperly receiving AFDC or Black Lung benefits and to identify program weaknesses requiring corrective action. Set forth below is the information required by paragraph 5.f.1 of the Revised Supplemental Guidance for Conducting Computerized Matching Programs issued by the Office of Management and Budget, 47 FR 21656 (May 19, 1982). A copy of this notice has been provided to both Houses of Congress and the Office of Management and Budget.

Dated: August 13, 1982.

Richard P. Kusserow,

Inspector General.

Report of Matching Program: Federal Personnel Records/AFDC and Black Lung Benefit Records

a. *Authority:* Pub. L. 94-505.

b. *Program Description:* 1. *AFDC Match.* The Office of Inspector General plans to match lists of AFDC recipients furnished by the various states against wage and/or annuity data of Federal employees, retirees, or survivors. Matches of identical factors ("hits") will be provided to appropriate federal, state, or local officials for further review and investigation. Where appropriate, federal officials will be requested to furnish wage data of Federal employees to States in which AFDC recipients reside. The appropriate States will review the individual "hits" and report the results of their findings and resolutions to the Office of Inspector General.

2. *Black Lung Match.* An extract of individuals (name, social security number, and date of birth) whose wages affect black lung benefit payments and who are in current payment status as shown on SSA's Black Lung Payment System will be matched against federal personnel records. Information from the Black Lung records which matches a beneficiary who is a Federal employee, retiree, or survivor will be identified as part of a computer print-out. The identifying information on these cases will be given to SSA for verification of the eligibility of the Black Lung beneficiaries to determine whether these beneficiaries have wages which may offset their benefit.

c. *Records to be Matched:* Records from the following records systems will be matched against state AFDC record tapes and the SSA Black Lung Payment System, 46 FR 52962 (October 27, 1981):

1. Office of Personnel Management—General Personnel Records system, 47 FR 16480 (April 16, 1982) and Civil Service Retirement and Insurance Records system, 47 FR 16474 (April 16, 1982)

2. Department of Defense, Defense Manpower Center Data Base system, 47 FR 16160 (April 15, 1982)

3. Tennessee Valley Authority-Personnel Records system, 45 FR 9429 (February 12, 1980); Payroll Records system, 45 FR 9435 (February 12, 1980); and Retirement Systems Record system, 45 FR 9445 (February 12, 1980)

4. Coast Guard, Active Duty Military Payroll System 46 FR 59752 (December 7, 1981) and Personnel Management Information System 46 FR 59750 (December 7, 1981)

Appropriate routine uses have been published by these agencies to permit disclosures to the Department to conduct these matches.

d. *Period of the Match:* These matches will begin in September and October, 1982 and will be completed within 6 months.

e. *Safeguards:* Records used in this match will be maintained under strict security. Access to the computer files and printed information is restricted to only those persons associated with the matching program on a "need-to-know" basis. The records will be kept in locked file cabinets and under the control of the Office of the Inspector General. We will return all of the computer source tapes to the respective sources within 60 days of the match. We will also degauss all computer work tapes at completion of the matching program. We protect all computer tapes by the use of passwords to prohibit unauthorized access. All computer files are safeguarded in accordance with the provisions of the National Bureau of Standards Federal Information Processing Standards 41 and HHS ADP Systems Manual, Part 6, "ADP Systems Security".

f. *Retention and Disposition of Records:* Only those records produced in the match which meet predetermined criteria will be maintained. All records maintained will be destroyed within 6 months except for those records which are necessary to the completion of pending law enforcement activities or administrative activities of the matching program. Paper listings will either be shredded or burned.

[FR Doc. 82-[illegible] Filed [illegible]; 8:45 am]

BILLING CODE [illegible]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Social Security Administration

Privacy Act of 1974; Report of New Matching Program

AGENCY: Social Security Administration, Health and Human Services Department.

ACTION: Notice of a Matching Program—Social Security Administration (SSA)/Department of Labor (DOL).

SUMMARY: SSA is issuing public notice of its intent to conduct a matching program with DOL. SSA, Office of System Requirements, will perform the match using certain data provided by DOL. The matching program will be an interface between an extract from DOL's Office of Worker's Compensation Programs Black Lung Claimant Information File (Federal Register, dated July 13, 1982, page 30065) and SSA's Master Beneficiary Record (MBR) (Federal Register, dated October 13, 1982, pages 45626–45628). The purpose of the match is to detect and/or prevent overpayments of SSA benefits.

DATE: Data exchange will begin in fiscal year 1983 and, unless comments are received which will result in a contrary determination, will recur periodically.

ADDRESS: Interested individuals may comment on this proposal by writing to the Privacy Officer, Social Security Administration, 6401 Security Boulevard, Baltimore, Maryland 21235. All comments received will be available for public inspection at 3-F-1 Operations Building at the above address.

FOR FURTHER INFORMATION CONTACT: Mr. Frank Bowings, Chief, Disability Systems Branch, Office of System Requirements, 3-M-11 Operations Building, Social Security Administration, 6401 Security Boulevard, Baltimore, Maryland 21235, area code (301) 594-8818.

SUPPLEMENTARY INFORMATION: The matching program which SSA will conduct will be a computerized interface between an extract from DOL's Office of Worker's Compensation Programs Black Lung Claimant Information File (Federal Register, dated July 13, 1982, page 30065) and SSA's MBR (Federal Register, dated October 13, 1982, pages 45626–45628). The purpose of the match is to detect and/or prevent overpayments of SSA benefits. DOL pays Part C Black Lung benefits to individuals who may also receive title II disability benefits. Part C payments come within the purview of section 224 of the Social Security Act and must be considered the same as other workmen's compensation payments in applying an offset to Social Security benefits. Since SSA offsets the beneficiary's disability benefits by the amount of the Part C Black Lung benefit, SSA will conduct a matching operation with DOL to detect and/or prevent overpayments of SSA benefits.

Presently, Black Lung Part C data are obtained through voluntary reporting by beneficiaries. Very often, beneficiaries claim to be unaware of the need to report initial receipt of, or changes in, Part C Black Lung benefits. SSA is, therefore, unable to make a timely and proper offset of benefits, thus creating an overpayment. Obtaining Part C Black Lung benefit data through a matching operation with DOL will permit timely, proper payment of disability benefits and detect and/or prevent overpayments.

Further information regarding the matching program including the authority for the program, a description of the program, the personal records to be matched, the dates of the program, security safeguards, and plans for disposition of the records are provided in the text below. This information is required by paragraph 5.f.1. of the Revised Supplemental Guidance for Conducting Matching Programs (Federal Register, May 19, 1982, pages 21657–21658). A copy of this notice has been provided to both Houses of Congress and the Office of Management and Budget.

Dated: April 13, 1983.

John A. Svahn,

Commissioner of Social Security.

Report of a Matching Program Social Security Administration Matching with Department of Labor Records

a. *Authority:* Section 224 of the Social Security Act.

b. *Description of Matching Program:*

1. *Organizations Involved:* The Social Security Administration (SSA) and the Department of Labor (DOL) are the involved components.

2. *Purpose:* DOL pays Part C Black Lung benefits to individuals who may also receive title II disability benefits. Part C payments come within the purview of section 224 of the Social Security Act and must be considered the same as other worker's compensation payments in applying an offset to Social Security benefits. Since SSA offsets the beneficiary's disability benefit by the amount of Part C Black Lung benefit, SSA will conduct a matching operation with DOL to prevent and/or detect overpayments. Presently, Black Lung Part C DOL data are obtained through voluntary reporting by beneficiaries. Very often, beneficiaries claim to be unaware of the need to report changes in the amount or initial receipt of Part C Black Lung benefits. Obtaining Part C Black Lung benefit data through a matching operation with DOL will give SSA relevant information earlier and permit more timely action to detect and prevent overpayments of SSA benefits.

3. *Procedures:* DOL will furnish SSA an extract file containing: Social Security number, name, current benefit amount data, effective date, date of birth, date of entitlement, and payment status of all Part C beneficiaries. This file will be processed against SSA's record of all title II beneficiaries. For those records matched, action will be taken to assure disability benefits are offset appropriately. SSA will make no subsequent contacts as part of this

matching program with DOL after DOL furnishes the extract file, except in specific cases where there is an inconsistency.

c. *Records to be Matched:* SSA will match the Master Beneficiary Record (MBR) [HHS/SSA/OURV 09-60-0090, Federal Register dated October 13, 1982, pages 45626–45628], which contains all data pertinent to the payment of Social Security recipients, with an extract from DOL, Office of Worker's Compensation Programs Black Lung Claimant Information File [DOL/ESA-6, Federal Register dated July 13, 1982, page 30365].

d. *Projected Starting and Ending Dates:* The match will begin in fiscal year 1983 and will be a continuing process except that subseqent files from DOL will contain only changes on previously reported individuals and additions of newly entitled Black Lung recipients.

e. *Security Safeguards:* Security safeguards pertaining to the MBR as reflected in the Federal Register dated October 13, 1982, pages 45626–45628, will apply. All magnetic tapes and discs are within an enclosure attended by security guards. Anyone entering or leaving this enclosure must have special badges which are issued only to authorized personnel. The same safeguards will apply to DOL tapes while they are in the possession of SSA. All microfilm and paper files are accessible only by authorized personnel with a need to know.

f. *Disposition of Records:* Data received will be returned to DOL after the matching operation. Information regarding "hits" will be incorporated into the MBR as necessary.

g. *Other Comments:* For those records matched, SSA will take proper action to assure that disability benefits are offset appropriately.

[FR Doc. 83-[illegible] Filed 4-19-83; 8:45 am]

BILLING CODE 4190-11-M

VETERANS ADMINISTRATION

Computer Matching Program; Federal Personnel Indebted to the Veterans Administration

AGENCY: Veterans Administration.

ACTION: Notice.

SUMMARY: Notice is hereby given that the VA OIG (Veterans Administration Office of Inspector General), in coordination with other Federal agencies, is conducting a series of computer matches as part of the VA's participation in the President's Council on Integrity and Efficiency Project entitled "Federal Employees Receiving Government Assistance." The matches will compare various Federal military and civilian personnel records with certain VA program records for the purpose of identifying and locating Federal personnel who currently are indebted to the VA or have received VA benefits to which they are not entitled. The goals of the matches are to reduce the amount of outstanding debt owed by individuals to the VA, to identify and eliminate the methods by which individuals obtain benefits without entitlement, and to recoup the dollar-value of received benefits from individuals who were not entitled to the benefits. Administrative, personnel, and civil actions, as appropriate, will be used by the VA during the collection process which will follow the matches. For the information of all concerned, the text of the VA matching program report, describing these computer matches, follows. In accordance with the OMB Matching Guidelines, dated May 11, 1982, copies of this report have been sent to OMB and both Houses of Congress.

FOR FURTHER INFORMATION CONTACT: Jim Durnil, (202) 389-2901.

Dated: August 23, 1982.

By direction of the Administrator.

Everett Alvarez, Jr.,
Deputy Administrator.

Veterans Administration, Office of Inspector General

Computer Matching Program: Federal Personnel Indebted to the Veterans Administration

Authority for and Purpose of the Program: The OIG (Office of Inspector General), pursuant to the authority granted by the Inspector General Act of 1978 (Pub. L. 95-452), has initiated a computer matching program. This program is designed to identify Federal personnel who have defaulted on VA loans or who have been provided VA benefits erroneously and from whom VA has been unable to collect. For purposes of this matching program, the term "Federal Personnel" includes Federal civilian employees and retirees; U.S. Armed Forces active duty personnel, retirees, and reservists; and survivors/beneficiaries of individuals in any of these categories.

Description of the Matching Program: This matching program will involve computer matches of Federal personnel data files from OPM (Office of Personnel Management), DOD (Department of Defense), TVA (Tennessee Valley Authority), and USCG (U.S. Coast Guard) with five VA program files described below. The VA program files are from two major program areas: Veterans Benefits Programs managed by the DVB (Department of Veteran Benefits) and Medical Service Programs managed by the DMAS (Department of Medicine and Surgery).

Files to be used in this matching program are: a. Veterans Administration:

(1) Patient Medical Records—VA (24 VA 136), 42 FR 49738.

(2) Compensation, Pension, Education and Rehabilitation Records—VA (58 VA 21/22/28), 47 FR 272.

(3) Loan Guaranty Home, Condominium, Mobile Home Loan Applicant Records and Paraplegic Grant Applications Records—VA (55 VA 26), 42 FR 49726.

(4) Veterans, Beneficiaries and Attorneys U.S. Government Insurance Award Records—VA (46 VA 00), 47 FR 29432.

(5) Veterans and Armed Forces Personnel U.S. Government In-Force Life Insurance Records—VA (36 VA 00), 47 FR 29432.

(6) Veterans and Beneficiaries Identification and Records Location Subsystem—VA (38 VA 23), 47 FR 388.

b. Office of Personnel Management:

(1) General Personnel Records System (OPM/GOVT-1), specifically the Central Personnel Data File (CPDF) within this system of records, 45 FR 79415 et seq.

(2) Civil Service Retirement and Insurance Records System (OPM/Central-1), specifically the Civil Service Retirement and Insurance File within this system of records, 46 FR 79415 et seq.

c. Department of Defense (Defense Logistics Agency):

Defense Manpower Data Center Data Base (S322.10 DLA–LZ), 47 FR 2844.

d. Department of Transportation (U.S. Coast Guard):

(1) Active Duty Military Payroll System (DOT/CG 523), 46 FR 38752.

(2) Personnel Management Information System (DOT/CG 624), 46 FR 38768.

e. Tennessee Valley Authority:

(1) Personnel Files (TVA–2), 46 FR 62983.

(2) Payroll Records (TVA–11), 46 FR 62983.

(3) Retirement System Records (TVA–20), 46 FR 62983. Objectives to be Met by the Matching Program:

The objectives of this matching program are to detect and identify Federal employees, retirees, or their survivors who have defaulted on VA loans or who have been provided VA benefits in error, and to provide sufficient locator information to permit initiation of collection or recoupment actions. While this program has been established as a one-time matching project, analysis of the results may support changing one or more of the individual matches to recurring projects.

Procedures of Matching Program: Step 1. Acquisition of Data Files. The four source agencies will provide the VA OIG computer tapes containing personal information on Federal personnel. DVB and DM&S will make available to the OIG copies of automated program files containing information about persons on the compensation, pension, education, accounts receivable, insurance award, guaranteed/insured loan, and patient treatment systems. All files will be safeguarded in accordance with the National Bureau of Standards' *Federal Information Processing Standards 41 and 31.* The information provided to the OIG will be acquired, controlled, and used in compliance with the Privacy Act of 1974 (5 U.S.C. 552a), 38 U.S.C. 3301 and 4132, implementing VA regulations, and the OMB Matching Guidelines, dated May 11, 1982.

Step 2. Computer Processing. The OIG Office of Audit will conduct the computer matching of the files. Results of the matches will be turned over to DVB or DM&S, as appropriate, for followup action.

Step 3. Routine Collection. DVB and DM&S will review the products of the match to determine the individuals for whom collection procedures should be initiated or reopened. VA will attempt to contact these individuals to try to resolve the accounts. VA will work with those responding who deny or dispute the liability.

Step 4. Federal Employee Assistance. VA will take the following actions concerning Federal employees who fail to respond to direct contact attempts:

(a) A letter will be sent to the debtor at his or her Federal employing agency requesting that the person immediately contact the VA. PERSONAL/PRIVATE—TO BE OPENED BY ADDRESSEE ONLY will be stamped in a prominent location on the envelope. The envelope will also contain a request that a forwarding address be furnished if the letter is undeliverable as addressed.

(b) Each federally employed debtor will have 60 days to respond. If the debtor is still nonresponsive, the employing agency will be asked to contact the employee about his or her indebtedness. With the concurrence of the VA General Counsel, a listing of those debtors for whom personal contact is being requested will be provided to the responsible administrative office for the employing agency.

Step 5. Litigation. The merits of each claim remaining unresolved will be reviewed and, if appropriate, the claim will be referred for followup action by a U.S. Attorney or VA District Counsel. Where there are reasonable grounds to believe there has been a violation of criminal law, the matter will be referred to the appropriate authorities for investigation and consideration of criminal prosecution.

Step 6. Records Maintained by DVB and DM&S. Any manual records resulting from the match will be maintained by DVB and DM&S. As claims are settled or repaid, the various files will be updated to reflect these changes.

Date of Matching Program: In accordance with the OMB Matching Guidelines, the computer matches were initiated after the publication of the routine use notices for all systems of records involved in the matching program. The match programs and referral of cases to DVB and DM&S should be completed during Fiscal Year 1982. The period of time which will be required by DVB and DM&S for completion of collection actions cannot be determined.

Disclosure of Records: a. VA Systems of Records Extracts to OIG. The transfer of extracts from the five VA Systems of Records to the OIG for performing the matches is an intra-agency "need-to-know" disclosure permitted under 5 U.S.C. 552a(b)(1) and is consistent with the statutory language creating the OIG which is found in Section 6(a)(1) of Public Law 95–452.

b. Source Agency Records to OIG. The transfer of extracts from the personnel files of the four source agencies to the OIG for performance of the matches will be carried out pursuant to the agencies' publications of routine use notices in the Federal Register. On completion of the match program, source agency files will be returned to their originators or electronically erased to prevent further access.

c. Transfer of Match Products from OIG to DVB and DM&S. The transfer of the products of the match (e.g., name, SSN, date of birth of the potential debtor) from the VA OIG to DVB and DM&S is an intra-agency, "need-to-know" disclosure permitted under 5 U.S.C. 552a(b)(1). Valid match information will become part of the appropriate VA system of records. Invalid match information will be erased or destroyed.

d. VA Request for Personnel Contact by Federal Employing Agencies. The transfer of information between VA and Federal employing agencies to permit personal contact of Federal employees is pursuant to the routine uses published in the Federal Register for the five VA systems of records.

e. Referral of Claims for Litigation. As appropriate, cases will be referred to U.S. Attorneys or VA District Counsels for the respective agency systems of records.

Efforts Taken to Protect Against Unauthorized Access to or Disclosure of Personal Records: a. The procedures set forth for the implementation of the proposed matching program incorporate (1) strong provisions to assure that the information disclosed is adequately safeguarded and that unwarranted disclosures do not occur, and (2) existing statutes and regulations regarding indebtedness of Federal employees.

b. Federal personnel identified as potentially receiving benefits without entitlement will have their eligibility for and receipt of VA benefits verified by DVB and DM&S, and those determined to be eligible for the benefits they are receiving will have no information disclosed from their records. Federal personnel identified as being in debt to the VA but in satisfactory adherence to repayment plans will have no information disclosed from their records. VA regulations and 38 U.S.C. 3102 and 4005a provide for waiver and subsequent appeal by any individual who feels that an appeal is warranted. Every effort will be made to ensure that each individual's personal and privacy rights are protected.

[FR Doc. [illegible] Filed [illegible]]

BILLING CODE [illegible]

WILLIAM V ROTH JR DELAWARE CHAIRMAN

TED STEVENS ALASKA
CHARLES McC MATHIAS JR MARYLAND
WILLIAM S COHEN MAINE
DAVE DURENBERGER MINNESOTA
WARREN B RUDMAN NEW HAMPSHIRE
THAD COCHRAN MISSISSIPPI

THOMAS F EAGLETON MISSOURI
LAWTON CHILES FLORIDA
SAM NUNN GEORGIA
JOHN GLENN OHIO
CARL LEVIN MICHIGAN
ALBERT GORE JR TENNESSEE

FRANKLIN G POLK CHIEF COUNSEL AND STAFF DIRECTOR
MARGARET P CRENSHAW MINORITY STAFF DIRECTOR

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
SUBCOMMITTEE ON
OVERSIGHT OF GOVERNMENT MANAGEMENT
WASHINGTON, DC 20510

SUBCOMMITTEE
WILLIAM S COHEN MAINE CHAIRMAN

WARREN B RUDMAN NEW HAMPSHIRE
DAVE DURENBERGER MINNESOTA

CARL LEVIN MICHIGAN
LAWTON CHILES FLORIDA

SUSAN M COLLINS STAFF DIRECTOR

September 19, 1986

The Honorable Joseph R. Wright, Jr.
Deputy Director
Office of Management and Budget
Executive Office Building
Washington, D.C. 20503

Dear Joe:

I want to thank you for testifying before the Subcommittee on Oversight of Government Management on S. 2756, the Computer Matching and Privacy Protection Act of 1986. As soon as the printed hearing record is available, I will see that a copy is sent to you.

As you will recall, at the hearing Senator Levin asked you to provide additional material for the record. Specifically, please provide the Subcommittee with the following statistics on matching programs that have been performed by federal agencies:

an inventory of the matching programs that have been performed;

the number of raw hits that were produced in these matching programs;

the number and percentage of raw hits that were independently verified;

the number of hits identified by the matches that actually resulted in savings or recovery to the federal government; and

the dollar savings resulting from the matching programs.

Again, thank you for your testimony and the assistance of you and your staff to the Subcommittee in our examination of these issues.

With best wishes, I am

Sincerely,

Bill

William S. Cohen
Chairman

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

OCT 07 1986

OCT 9 1986

Honorable William S. Cohen
Chairman, Subcommittee on Oversight
of Government Management
Committee on Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

I was pleased to have the chance to testify on your computer matching bill, S. 2756. Matching is an area in which I am very much interested, both from the standpoint of encouraging governmental efficiency as well as protecting individuals' privacy. Hearings such as yours which serve to focus attention on these issues are both useful and welcome.

I am enclosing some of the supplemental material for-the-record that we agreed to provide in response to Senator Levin's request. Specifically, you will find an inventory of all of the matching programs reported to OMB pursuant to both our 1979 and 1982 Guidelines. You should note that this does not represent a complete inventory of all matching done by the Federal Government since the Guidelines exclude certain types of matches from their reporting requirements, e.g., front-end eligibility verifications, routine financial matches done for administrative purposes, matches in which the Federal participant was a matching source only, and the like.

To provide an additional perspective on the scope of matching in general, I am also enclosing a copy of a survey of State front-end eligibility matching efforts prepared as a project of the President's Council on Integrity and Efficiency (PCIE). The survey was intended to catalog the varieties of automated techniques in use by the States in order to help any States considering implementing front-end verification processes or enhancing their existing ones; it was not meant to be a comprehensive listing of all such programs.

We are currently gathering information that will be responsive to the remainder of Senator Levin's request relating to "raw hits" and "dollar savings." In order to provide these data in a timely fashion, we have sought data only for calendar years 1985 and 1986, on the theory that agencies are more likely to have information about current programs readily at hand. We will provide these data as soon as they are available.

As I said at the hearing, we look forward to working with you and your staff on this important effort.

Sincerely,

Joseph R. Wright, Jr.
Deputy Director

Enclosures

INVENTORY OF MATCHING PROGRAMS
SUBMITTED TO THE OFFICE OF MANAGEMENT AND BUDGET
UNDER GUIDELINES ISSUED IN 1979 AND REVISED IN 1982

Submitting Agency	Date Submitted	Description of Matching Program
Commerce	6/27/79	Bureau of Census statistical data not containing personal identifiers.
Railroad Retirement Board	6/28/79	Negative report.
Veterans Administration	7/11/79	Employee Accounts Receivable System Program Post Vietnam Era Veterans' Educational Assistance Program VAPAID System Matching Program
Health Education and Welfare	7/9/79	(1) GSA employee records with GSA. (2) DOD military retirees with SSI recipients. (3) VA compensation and benefit records with SSI recipients. (4) OPM annuitant and survivor benefits records with SSI recipients. (5) RRB annuitant and survivor benefit records with SSI recipients. (6) OE BEOG student application records with SSA student beneficiaries. (7) OE BEOG payment records with SSA student beneficiaries. (8) OE State Guarantee Agency Student Loan Default file with HEW personnel file.
Veterans Administration	7/31/80	Matching report
Defense	7/18/80	Matching - Recon of DOD and VA Records with respect to Mil Annuities, Res Pay and VA Disability Indemn Com.
Veterans Administration	7/31/80	Compensation/Pension and Education Match.

Postal Service	11/14/80	Personnel Records Injury Compensation Validation Records. Personnel Records -- Office of Workers' Comp Program (Amended)
Agriculture	7/13/81	Matching reports on Computer Matching of USDA Employees Against Illinois Department of Registration and Education Master File for Real Estate Brokers and Sales Persons
Health and Human Services	5/19/81	Matching of HHS payroll records with Social Security Administration Master Files of SSN.
Housing and Urban Development	4/1/82	Matching report titled "Assisted Housing Program Matching Report".
Defense	6/18/82	Copy of a notice for a computer matching program.
Health and Human Services	8/16/82	Matching program (new) in accordance with Guidance for Matching Programs published in the Federal Register, May 19, 1982 SSA Matching with Office of Personnel Management Records.
Commissioner of Social Security	4/18/83	Matching program in accordance with OMB Revised Supplemental Guidance for Matching Programs published in the Federal Register on May 19, 1982 (SSA/DOL).
Justice	4/23/83	Matching program to involve computer matches of data contained in the NCIC Wanted and Missing Person File records with data contained in various Federal, State, and local agency data bases.
Housing and Urban Development	4/2/83	Matching program with the objective of obtaining salary and benefit attachments to discharge debts owed to the U.S. Government.
Defense	7/17/83	Matching program to involve manpower records of the Department of Defense and the Central Personnel Data File

		and civil Service Retiree File of the Office of Personnel Management.
Agriculture	8/8/83	Matching to perform wage match of FmHA tenants in the State of Virginia, against the wage files of the VEC to detect underreporting of income in order to receive higher mortgage interest subsidies or rent subsidies.
Selective Service System	9/7/83	Matching program to locate absent parents with child support obligations.
Office of Personnel Management	12/2/83	Matching program to have agencies update their beneficiary data maintained in the agencies' master records.
NASA	12/30/83	Matching program to match automated records of the U.S. Department of Labor for Federal Employees' Compensation Act claims with automated personnel records of NASA Langley Research Center personnel. The objective is to analyze environmental and occupational conditions of hearing loss claimants to possibly identify the causes for the rise in hearing loss claims at Langley Research Center.
Defense	1/1/84	Matching program to involve allotment records of the Department of the Navy and food stamp and public assistance records of the City of New York.
Veterans Administration	1/4/84	Matching program to identify the unwarranted payment of VA pension and certain compensation benefits which results when beneficiaries fail to report earned income.
Veterans Administration	1/4/84	Matching program to match lists of veterans and beneficiaries no received compensation, DIC or pension benefits from the VA with records of Federal, State and local correctional organizations to identify recipients who may be ineligible to receive these

		benefits. The ineligibility may occur when the VA has not been informed of the incarceration of the individual for a period of more than 60 days following his/her conviction for a felony, or for a misdemeanor or felony in the case of a pension recipient.
Selective Service System	2/29/84	Matching program to identify Registration Violators.
Commissioner of Social Security	7/23/84	Matching program to involve the State of California's "599 File". The 599 file is maintained by the California Franchise Tax Board, based on data reported by finanical institutions throughout the State.
Postal Service	7/24/84	Matching program to identify recipients of benefits under those programs who are employed by the Postal Services and have not reported their earnings as a result of such employment to DC-DHS.
Transportation	8/13/84	Matching program to match a system or records for the RRB in Chicago to an employment file from the Pennsylvania Department of Labor and Industry.
Health and Human Services	9/7/84	Matching program to conduct matches of Federal, State and local government personnel records with Social Security benefit records. The title is "Federal, State and Local Government Personnel Records/Social Security Beneficiary Records."
Selective Service System	9/25/84	Matching program to identify registration violators. Concerns revision of the SSS Registration Compliance Program for computerized matching of individual records maintained by SSS.
Veterans Administration	11/26	Matching program to detect unwarranted compensation, pension, death compensation, dependency and indemnity compensation, non-service-connected death pension

		payments or educational assistance benefits that may have been provided to non-entitled veterans or ineligible spouses of disabled or deceased veterans. This ineligibility or non-entitlement may occur as a result of the remarriage of a surviving spouse of a deceased veteran or the divorce or annulment of the marriage of a veteran and spouse.
Defense	12/14/84	Matching program will involve records of the Manpower Data Center, Department of Defense and the U.S. Coast Guard, Department of Transportation, being matched with records from the Veterans Administration's (VA) benefit payment data. The purpose is to identify those members of the active Reserve Forces who are also receiving VA pensions or compensation.
Commissioner of Social Services	1/29/85	Matching program will be an interface involving SSA's Master Beneficiary Record (MBR), the Supplemental Security Income Record (SSR), and the Black Lung Payment System matched against extracts of the WC payment files maintained by the State agencies and the DOL system of records. The purpose of the match is to detect and/or prevent erroneous payments of SSA benefits.
Defense	3/11/85	Matching program by the Marine Corps entails matching a tape furnished by the City of New York listing the names and addresses of all current public assistance/food stamp recipients against a tape listing Marine Corps allotments paid to named recipients in New York City. Any "hits" will be furnished to the City of New York which independently may determine whether the recipient meets the threshold eligibility requirements for aid provided by the city. (MFD00004, "Bond and

		Allotment (B&A) System").
Defense	3/28/85	Matching program between the Department of Defense and the U.S. Postal Service to identify those Postal Service employees who are indebted to the United States under programs administered by the Department of Defense. The records provided by the Postal Service will be matched with the Department of Defense debtor records and the hits will be referred to the Postal Service which will provide the home and work address of each debtor to the Department of Defense. These records will be used to contact the debtor to request payment of the debt. A further match of the Postal Service records with the DOD Reserve Forces records will be done in order to identify those Postal Service employees who are reservists. This will allow the PS to identify employees who would be critical to the PS in time of national emergency and shouldn't be in the Ready Reserve.
Railroad Retirement Board	4/19/85	Matching program for the VA to furnish the RRB with an extract file from the VA Compensation and Pension (C&P) master file. An extract record will be prepared for each VA beneficiary who is receiving income-dependent benefits (Pension or parent DIC).
Health and Human Services	5/2/85	Matching program entitled "HHS Personnel Records/Federal Bureau of Investigation Identification Records." This match is of HHS employees identified as holding positions involving access to financial or benefit payment systems and/or involving automated data processing against Federal Bureau of Investigation identification records on arrests and convictions to verify information supplied by the employees on Personal Qualifications Statements (SF-171s) and to up-date information on convictions. Raw

		hits will be reviewed and verified as necessary with Federal, State, and local law enforcement agencies.
Veterans Administration	4/29/85	Matching program entitled "Veterans Administration Records of Physicians, Dentists and Other Health Care Professionals/State Licensing Records." This match is to verify that physicians, dentists, podiatrists, optometrists, and psychologists employed or utilized by the agency are holding current, unrestricted licenses to practice and that nurses and pharmacists are registered in a State.
Veterans Administration	5/31/85	Department of Veterans Benefits will conduct a series of recurring computer matches of VA compensation, pension, education, rehabilitation and home loan default indebtness records with Office of Personnel Management's Central Personnel Data File.
Office of Personnel Management	7/1/85	Matching program to be conducted by OPM and OWCP to identify individuals receiving concurrent benefits under the Civil Service Retirement Act (CSRA) and the Federal Employees' Compensation Act (FECA).
Veterans Administration	7/25/85	Matching program to be conducted by the Office of the IG. Will conduct a series of computer matches of VA records of physicians and dentists with Federal, State, local and private income and payment records. The goal of these matches is to identify full-time physicians and dentists who may have engaged in unauthorized outside professional activities, or received unreported remuneration for their outside professional activities.
Veterans Administration	7/25/85	Matching program to be conducted by the Office of IG with a series of computer matches of VA records of physicians, dentists, and other health care professionals with

		Federal, State, local and private organizations maintaining licensure and registration records. The goal of these matches is to verify that physicians, dentists, podiatrists, optometrists, and physchologists employed or utilized by the Agency are holding current, unrestricted licenses to practice and that nurses and pharmacists are registered in a State.
Veterans Administration	8/26/85	Matching program to be conducted by the VA. The VA intends to conduct a recurring computer matching program matching DOL and SSA records of Black Lung benefit recipients with VA pension and parents' dependency and indemnity compensation records. The goal of these matches is to identify VA benefit recipients who are also receiving Black Lung benefits payments reportable to VA as countable income.
Agriculture	8/27/85	Two matching programs to be conducted by the Department of Agriculture published in the Federal Register on December 10, 1984. These programs are aimed at reducing the Department's costs incurred in connection with unemployment compensation and workers' compensation.
Postal Service	9/11/85	Matching program to be conducted between the Postal Service and the Department of HUD. The Postal Service plans to match by computer certain records in its Payroll system file with the U.S. Department of HUD records on individuals receiving assisted housing benefits.
Postal Service	9/13/85	Three matching programs to be conducted by the Postal Service published in the Federal Register on May 1, 1985. (1) Match between the Postal Service and the Department of Agriculture. (2) Match between the Postal Service and the State of Indiana Employment Security

		Division. (3) Match between Postal Service and City of Philadelphia, and Philadelphia School District.
Agriculture	12/10/85	The OIG, Agriculture intends to conduct continuing matching programs to detect and prevent fraud and abuse in USDA programs. The matches will compare Farmers Home Administration loan files against the personnel data files of the Office of Personnel Management for the purpose of identifying Federal personnel data files of the OPM and various Federal personnel or VA pension records with certain Food Stamp Program records for the purpose of identifying Federal personnel who have received food stamp benefits to which they are not entitled.
Health and Human Services	1/8/86	Matching Program entitled "Verification of Licensure and Other Professional Credentials of PHS Health Professionals in the PHS Commissioned Corps and Civil Service Personnel."
Housing and Urban Development	1/28/86	HUD's Office of Inspector General will conduct or directly supervise computer matches of data on debtors having defaulted notes under section 312 of the Housing Act of 1964 against systems of records of current employees and retirees provided by the Office of Personnel Management, the United States Postal Service and the Department of Defense. The purpose of the program is to obtain salary and benefit attachments to discharge debts owed to the Federal Government.
Veterans Administration	3/27/86	The VA is providing notice that the Office of the Inspector General and the Department of Veterans Benefits will conduct a series of computer matches of VA compensation and pension records with Federal, State, and local records of incarcerated persons. The goal of these matches is to detect

		unwarranted compensation, dependency, and indemnity compensation (DIC), and pension payments made under Title 38.
Housing and Urban Development	5/1/86	HUD's HUD/Public Housing Agencies and Subsidized Multi-family Projects. HUD's Office of IG would conduct or directly supervise computer matches of tenant records at Public Housing Agencies and HUD-subsidized multi-family projects with various types of income data maintained by States and by the OPM.
Postal Service	5/9/86	Matching program sent to the Federal Register -- Postal Service/State of Missouri Department of Social Services.
Defense	6/13/86	Notice for new computer matching program submitted on 6/13 to Federal Register. Entails matching DoD records of civilian, active duty military, retired military and reserved military personnel with HUD records of individual assistance. Purpose to identify individuals receiving housing assistance who have income above amount necessary to receive benefits.
Defense	6/19/86	Entails matching DoD records of DoD employees with the source agency, HUD records of delinquent debtors who have Title I defaulted loans. Purpose to determine which debtors are current DoD employees so as to allow HUD to collect debts under the salary offset provisions of the Debt Collections Act of 1982.
Commissioner of Social Security Baltimore, Maryland	6/21/86	Social Security Administration (SSA) Matching with State Records Expansion of the State and Federal Exchange (SAFE) Program.
Defense	6/24/86	Entails matching data furnished by the VA identifying records of veterans and their dependents who are indebted to the Federal Government under the Debt Collection Act of 1982. The VA will be

		responsible for reviewing information supplied by BoD and for action to recover the outstanding debt(s) by salary or administrative offset, when other collection actions have been pursued and have been unsatisfactory.
Defense	8/13/86	Entails matching data furnished by the State Medicaid agencies of the 50 states and D.C. to identify the extent to which State Medicaid beneficiaries are eligible for Uniform Services health care benefits.
Veterans Administration	8/29/86	Goal of matches to identify active Postal employees, who are indebted to the VA under the compensation, pension, education and rehabilitation benefit programs or resulting from home loan defaults. Purpose of match to initiate salary offset in the collection of unpaid obligations to VA.
Veterans Administration	8/14/86	Intent by the Department of Veterans Benefits to match the BIRLS master records wtih readjustment or severance pay data records from Defense Manpower Data Center.
Veterans Administration	8/22/86	OIG will expand the series of computer matches it is conducting of VA compensation and Pension records with State and local wage, tax and employment security records.
Agriculture	9/12/86	Matching report entitled "Cross-State Wage, Unemployment Compensation, and Food Stamp Recipient Match of Food Stamp Program Participants in Oregon, Washington and Idaho.

CATALOG OF AUTOMATED FRONT-END ELIGIBILITY VERIFICATION TECHNIQUES

A Project of the President's Council on Integrity and Efficiency

PREPARED BY:

OFFICE OF INSPECTOR GENERAL
RICHARD P. KUSSEROW

U.S. DEPARTMENT OF HEALTH
AND HUMAN SERVICES

SEPTEMBER 1985

TABLE OF CONTENTS

FOREWORD i

SECTION I - BACKGROUND INFORMATION ON STUDY
Background 1
What Are Automated Front-End Eligibility Verification Systems? 1
Why Front-End Verification Techniques? 2
Parameters of This Catalog 2
Methodology of the Project 3

SECTION II - SUMMARY DATA FROM STATE SURVEYS
Location of Welfare Techniques 6
Location of Employment Security Techniques 7
Number of Techniques By State 8
Total Number of Techniques Verifying Eligibility Factors.. 10
Number of Techniques Verifying Eligibility Factors, By Program 11
Method of Computer Processing 13
Index of Techniques By Program, Factor Verified and Page Number 14

SECTION III - INDIVIDUAL TECHNIQUE DESCRIPTIONS [1]
Alabama 41-47
Alaska 48-49
Arizona 50-53
Arkansas 54-56
California 57-58
Colorado 59-64
Connecticut 65-67
Delaware 68-76
District of Columbia 77-83
Florida 84-87
Georgia 88-90
Hawaii 91-95
Idaho 96-99
Illinois 100-103
Indiana 104-108
Iowa 109-113
Kansas 114
Kentucky 115-116
Louisiana 117-118
Maine 119-122
Maryland 123-124
Massachusetts 125
Michigan 126-129
Mississippi 130-133
Missouri 134-138
Montana 139
Nevada 140-143
New Hampshire 144-146

[1] Materials in this section retained in the subcommittee files.

New Jersey 147-149
New Mexico 150-153
New York 154-157
North Carolina 158-164
North Dakota 165-166
Ohio 167
Oklahoma 168-169
Oregon 170-173
Pennsylvania 174-176
Puerto Rico 177
Rhode Island 178
South Carolina 179-180
Tennessee 181-182
Texas 183-192
Utah 193-194
Vermont 195-197
Virginia 198-200
Virgin Islands 201
Washington 202-204
Wisconsin 205-207
Wyoming 208-211
West Virginia 212-213

APPENDICES

A - Survey of Computerized Front-End Verification Techniques: State or Local Front-End Technique Profile 214

B - Glossary of Abbreviations and Terms 221

Foreword

This catalog highlights the results of a survey of State front-end or prepayment automated techniques used to verify eligibility for four major benefit programs: Aid to Families with Dependent Children, Food Stamps, Medicaid and Unemployment Insurance. The techniques reported here are used to prevent fraud and errors; i.e., they are used to confirm eligibility for benefits before any payments are made. The catalog has been compiled by the U.S. Department of Health and Human Services' Office of the Inspector General (OIG), under the aegis of the President's Council on Integrity and Efficiency, to promote the sharing of money-saving computer technology among all the States and U.S. territories.

The Deficit Reduction Act (DEFRA), signed by President Reagan in July 1984, includes new provisions on income and eligibility verification procedures. These procedures will directly affect how States confirm the eligibility of applicants for the benefit programs mentioned above. The new DEFRA provisions will enable federally funded welfare agencies to make more accurate eligibility determinations and benefit payments by exchanging information with each other and by obtaining unearned income data from the Internal Revenue Service and wage and other income information from the Social Security Administration. The techniques described in this catalog are employed at the front-end; many of them accomplish one or more of the goals mandated under DEFRA. Thus, this compendium will help States identify efficient, effective ways to comply with the income and eligibility verification regulations to be published in the near future.

By widely disseminating this comprehensive listing of preventive computer applications, we intend to assist those States and jurisdictions considering implementing front-end techniques or enhancing their systems. Although much attention has been given to computer techniques in recent years, this is the first national study to concentrate solely on prepayment use of automated verification systems. Our goal in publishing this catalog is to identify the increasing use of automated front-end verification applications and to offer possible systems for replication.

This catalog does not recommend one technique over another. Rather, it lists all current techniques and those under development. Section I includes background information and the study methodology. Section II presents summary data about the kinds and levels of front-end techniques reported by all 50 States, the District of Columbia and the jurisdictions of Guam, Puerto Rico and the Virgin Islands. Section III contains individual descriptions of the 173 different techniques reported as in use or under development by the jurisdictions. The appendices contain the survey which was sent to the States, and a glossary of abbreviations and terms.

This project would not have been possible without the participation of the States and territories surveyed. Thanks to their cooperation, we have been able to gather important data on a new preventive technology and thus help reduce fraud, waste and abuse in welfare and employment security programs.

This catalog is the product of many efforts over long months. During that time, I have chaired an interdisciplinary work group from the various Offices of Inspectors General and other organizations. Their contributions have been critical to compiling this catalog, which I am certain will promote the increased use of automated front-end verification techniques. I would like to thank the work group members: Mary Barry, Department of Housing and Urban Development; Allene Brown, Department of Education; Paula Hayes, Department of Agriculture; Les Johnson, Department of Agriculture; Doug Hunt, National Aeronautics and Space Administration; Virgil Jones, Department of Health and Human Services; Mike Marshall, Department of Agriculture; Pat Skees, Department of Labor; Pat Spirer, Department of Agriculture; and Clayton Vickland, D.C. Department of Human Services.

From my staff, Elisabeth Handley served as Project Director, with the help of Alana Landey, Assistant Director, Elsie Chaisson, Ed Meyers, Gail Shelton, Jane Tebbutt and Charlette Ross.

Additional copies of this catalog are available from the U.S. Department of Health and Human Services, Office of the Inspector General, Office of Analysis and Inspections, 330 Independence Avenue, S.W., Room 5643, Washington, D.C. 20201.

Richard P. Kusserow

Richard P. Kusserow
Inspector General

SECTION I - BACKGROUND INFORMATION ON STUDY

Background

Over the past several years, Federal and State governments have become heavily dependent on computers in many facets of their daily activities. Over 20,000 mainframe computerized systems have been identified in the Federal Government to date, and the number of State systems is growing at a rapid rate. This increased use of data processing is especially critical to the many public benefit programs, which distribute billions of dollars in public aid annually. In these times of decreasing resources, data processing technology provides program administrators with an opportunity to increase productivity while keeping operating costs constant.

One organization involved deeply in this issue is the President's Council on Integrity and Efficiency (PCIE). The PCIE, composed of Federal agency Inspectors General and chaired by the Deputy Director of the Office of Management and Budget (OMB), was created by President Reagan in March 1981 to coordinate Government-wide efforts to reduce fraud, waste and abuse. One of the PCIE's concerns is to encourage States to use computer technology in administering their benefit programs as one means of preventing overpayments and reducing welfare fraud. The Council has emphasized the use of "front-end" or "prepayment" techniques that are used to verify applicants' eligibility before they receive any payments, thus preventing overpayments and insuring that benefits reach only those entitled to them.

What Are Automated Front-End Eligibility Verification Systems?

An automated front-end eligibility verification system or technique, as we have defined it, is a method to ensure via computer that an applicant to a benefit program is entitled to the benefits before actual payment or award is made. An example would be a statewide network of computers containing data on State residents receiving unemployment compensation benefits, which are used by eligibility workers at the beginning of the eligibility determination process to determine if applicants are accurately reporting this type of income. No ruling on eligibility would be made and no benefits would be paid until the unemployment compensation benefit information has been received, analyzed, and verified. In benefit programs such as Aid to Families with Dependent Children (AFDC), Food Stamps and Medicaid, unearned income such as this is one of the keys to eligibility, and the fast and accurate verification of it is critical to preventing erroneous payments.

Eligibility factors other than unearned income can also be verified on the front-end. Other eligibility factors listed in this catalog include earned income, age, citizenship, identity, work history, and others. Regardless of which eligibility factors are verified, each technique in this catalog employs a computer to verify certain facts about applicants before benefits are awarded.

Why Front-End Verification Techniques?

The Federal Government is specifically interested in front-end or prepayment eligibility verification techniques because such techniques improve the efficiency and effectiveness of benefit programs and save money by preventing erroneous payments or overpayments. A preventive, proactive approach to the error and abuse in benefit programs can detect waste and prevent theft before those who have accidentally or intentionally misrepresented their circumstances receive payments.

While it is impossible to pinpoint the exact dollars saved via deterrence measures, effective deterrence is cost-beneficial given the expenses incurred through detecting and eliminating already-existing fraud and abuse. These costs include searching for and identifying crime, tracking the perpetrator, possible court costs, and often lengthy and ineffective collection procedures to recoup losses.

Automation especially lends itself to fraud prevention efforts, given its speed and accuracy. A computerized eligibility verification system can match or screen data in seconds, often while the applicant is still in the office. The Federal Government, via the PCIE, encourages the use of such techniques because automated front-end verification systems help avoid the expense of overpayments resulting from either applicant fraud or human mistake.

Parameters of This Catalog

This catalog lists automated front-end eligibility verification techniques currently used or under development for use in States' Aid to Families with Dependent Children, Food Stamp, Medicaid and Unemployment Insurance programs. These four programs were selected because they are among the largest in terms of people served and program expenditures. Also, since the project could not encompass all public assistance or benefit programs, we opted to focus on programs with high levels of public participation.

The catalog concentrates only on prepayment techniques because of their considerable prevention/deterrence effects outlined above. The project considers only automated verification systems because, although many manual front-end eligibility verification techniques are known to be in use, manual applications are labor-intensive and time-consuming. Project work group members agreed that the project's focus should be on the most efficient eligibility verification methods possible, i.e., automated methods.

Methodology of the Project

Our project goals were (1) to identify the level of State activity in automated front-end eligibility verification systems and (2) to encourage more States to use such systems. We decided to concentrate only on computer matches and screens because they are automated processes which involve the comparison of sets of data elements, either between two separate computer files (a match) or within the same file (a screen). Computers are the ideal method of performing routinized comparisons between extensive listings of data such as benefit program participants and new applicants, given the speed with which they can process vast amounts of information.

A category of automated front-end technique which we chose not to consider is the edit - a check in a system to assure that data elements entered are within certain acceptable limits. Edits are very commonplace and it would take considerable space to list the hundreds of routine edits used by the States. Also it appears that edits serve as threshold checks to prevent non-entry or inconsistent entry of data rather than to verify eligibility.

To complete the project, a questionnaire (see Appendix A) was formulated by work group members and survey design experts. A draft of the survey instrument was pretested in three States: Nevada, Texas and Maryland. The final survey instrument was mailed in late April 1984 to the heads of the departments administering the Aid to Families with Dependent Children, Food Stamp, Medicaid and Unemployment Insurance programs in each State and in the District of Columbia, Guam, Puerto Rico and the Virgin Islands. Thus, the techniques reflect information returned by State officials about State and local systems.

Returned surveys were compiled into a draft catalog which was distributed to State and Federal program officials for comments in March, 1985. After receiving their revisions, comments, and additional techniques, this final catalog was prepared. The techniques contained in it reflect only information supplied by State officials about State and local systems, and is current as of August 30, 1985. Eight agencies out of 109 did not respond to the initial survey or to the draft catalog. (The same eight did not respond to both the survey and the draft catalog). Thus, the catalog has a response rate of 93 percent.

We screened each returned survey for both the draft and final catalogs for whether it fit the definition of a front-end eligibility verification technique. In addition, we eliminated non-qualifying techniques, such as those involving automated eligibility determination processes instead of verification processes and those involving eligibility verification after receipt of benefits. Work group members made follow-up telephone calls to complete those surveys which lacked information or required clarification.

Some data from the surveys, such as cost effectiveness figures, are not listed in the individual descriptions in this catalog. Little information was supplied on these items, and what data we did get was usually incomplete - i.e., States told us how much a technique cost without providing savings figures, or they provided out-of-date numbers. On the other hand, there are data in the catalog's descriptions which were not requested on the survey form. This information was obtained either from the narrative descriptions provided by the States or in our follow-up telephone calls.

While we were very interested in collecting information on the impact of the individual techniques, the data provided by States were too incomplete to include. As Appendix A indicates, on the initial survey we asked States, for each technique, their developmental and operating costs, annual savings, annual number of applications denied, and numbers of raw and valid hits. For 54 of the 128 techniques, some information was provided for the eligibility verification techniques reported in the March 1985 draft catalog. The table below illustrates the paucity of consistent information across techniques:

For the draft catalog:

Information	Number of Techniques Reporting Data (Out of 128)
Developmental Costs	34 (27 percent)
Annual Operating Costs	27 (21 percent)
Annual Savings	13 (10 percent)
Number of Applications Denied Annually	16 (13 percent)
Number of Raw Hits	13 (10 percent)
Number of Valid Hits	10 (8 percent)

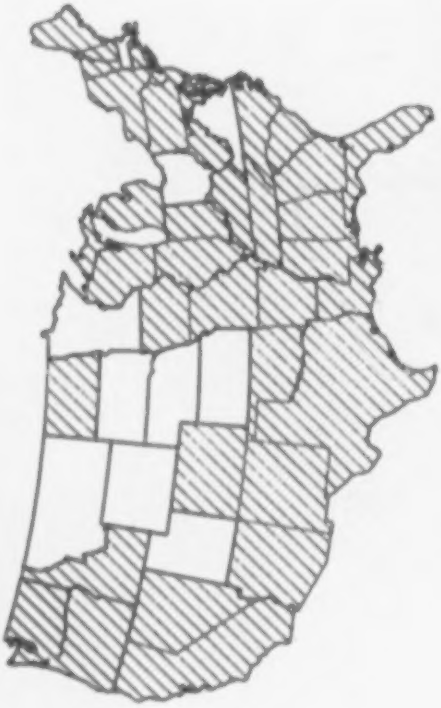
What this table does not show is how diverse responses were. States provided savings estimates without any operating cost estimates and vice versa. The figures themselves were in "old" dollars (i.e., a State might report developmental costs for

1976), and did not include the State's methodology for arriving at a particular number. For example, one agency estimated that it cost them $200 to develop and $10 annually to operate a system which verifies earned income. Another agency estimated that 98 percent of the hits they obtain from a check for duplicate benefits are valid. Clearly, further explanation is needed. Because of these difficulties, these data were not included.

SECTION II - SUMMARY DATA FROM THE SURVEYS

The data for the charts and tables which follow were extracted from the individual technique descriptions.

LOCATION OF WELFARE TECHNIQUES *

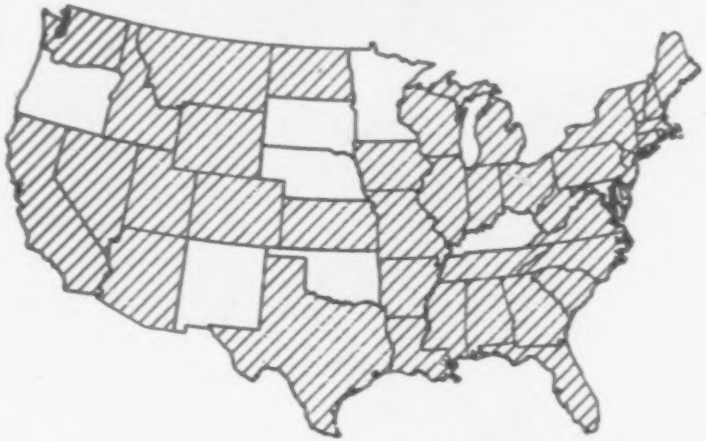


▨ One or more AFDC, Food Stamp or Medicaid Techniques In Operation or Under Development

☐ No AFDC, Food Stamp or Medicaid Techniques Reported. (This category includes survey nonrespondents.)

* Alaska and Hawaii each reported one or more AFDC, Food Stamp or Medicaid techniques. No welfare techniques were reported in Guam, Puerto Rico or the Virgin Islands.

LOCATION OF EMPLOYMENT SECURITY TECHNIQUES *



▨ One or more Unemployment Insurance Techniques In Operation or Under Development

☐ No Unemployment Insurance Techniques Reported. (This category includes survey nonrespondents.)

* Alaska, Puerto Rico and the Virgin Islands each reported one or more Unemployment Insurance techniques. Hawaii reported no Unemployment Insurance techniques. Guam does not have an Unemployment Insurance program.

NUMBER OF TECHNIQUES BY STATE

STATE	AGENCY	
	WELFARE*	EMPLOYMENT SECURITY
Alabama	5	2
Alaska	1	1
Arizona	3	1
Arkansas	2	1
California	1**	1
Colorado	3	3
Connecticut	2	1
Delaware	9	N/A***
District of Columbia	5	2
Florida	2	2
Georgia	1	2
Guam	0	0
Hawaii	5	0
Idaho	3	1
Illinois	1	3
Indiana	1	4
Iowa	4	1
Kansas	0	1
Kentucky	2	0
Louisiana	1	1
Maine	3	1
Maryland	2	0
Massachusetts	0	1
Michigan	2	2
Minnesota	0	0
Mississippi	1	3
Missouri	2	3
Montana	0	1
Nebraska	0	0
Nevada	3	1
New Hampshire	2	1
New Jersey	1	2
New Mexico	4	0
New York	2	2
North Carolina	6	1
North Dakota	1	1
Ohio	0	1
Oklahoma	2	0
Oregon	4	0
Pennsylvania	1	2
Puerto Rico	0****	1
Rhode Island	0	1
South Carolina	1	1
South Dakota	0	0

NUMBER OF TECHNIQUES BY STATE

STATE	AGENCY	
	WELFARE*	EMPLOYMENT SECURITY
Tennessee	1	1
Texas	5	5
Utah	N/A	2
Vermont	2	1
Virginia	N/A	3
Virgin Islands	0****	1
Washington	2	1
West Virginia	1	1
Wisconsin	1	2
Wyoming	0	4
	100	73

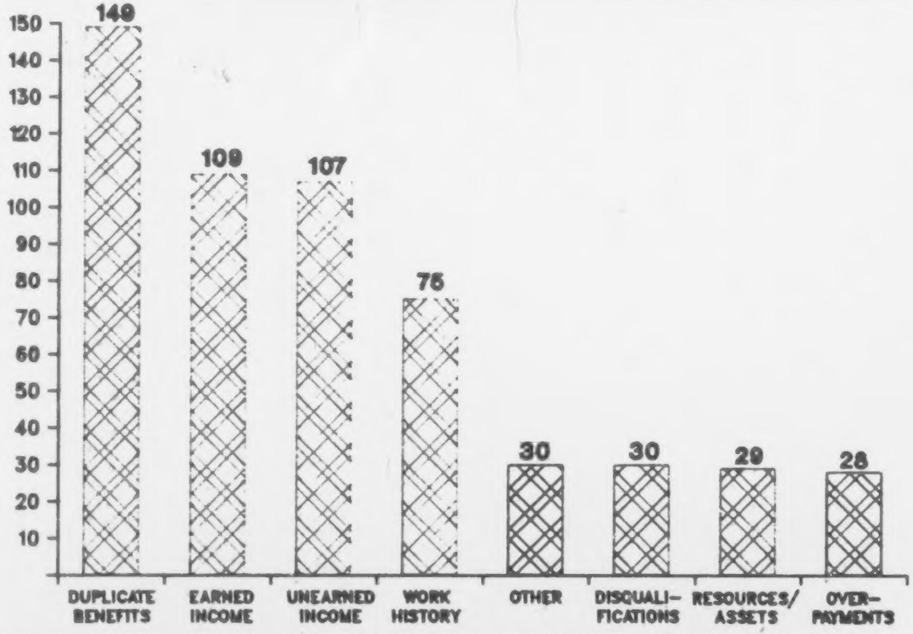
*Welfare refers to the agencies administering AFDC, Food Stamps, and Medicaid. Employment Security refers to the agencies administering Unemployment Insurance.

**The agency responsible for administering California's AFDC and Food Stamp programs did not respond to the survey or draft catalog.

***N/A means not available. Agencies with this listing did not respond to the survey or draft catalog. A zero indicates that an agency responded negatively.

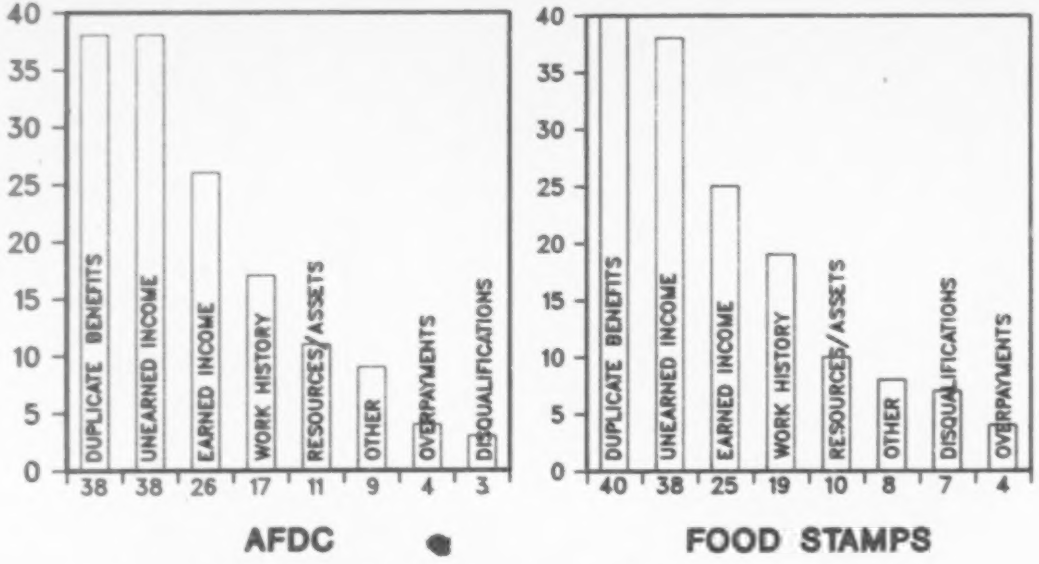
****The Puerto Rico and Virgin Island Medicaid agencies did not respond to the survey or draft catalog.

TOTAL NUMBER OF TECHNIQUES VERIFYING ELIGIBILITY FACTORS *



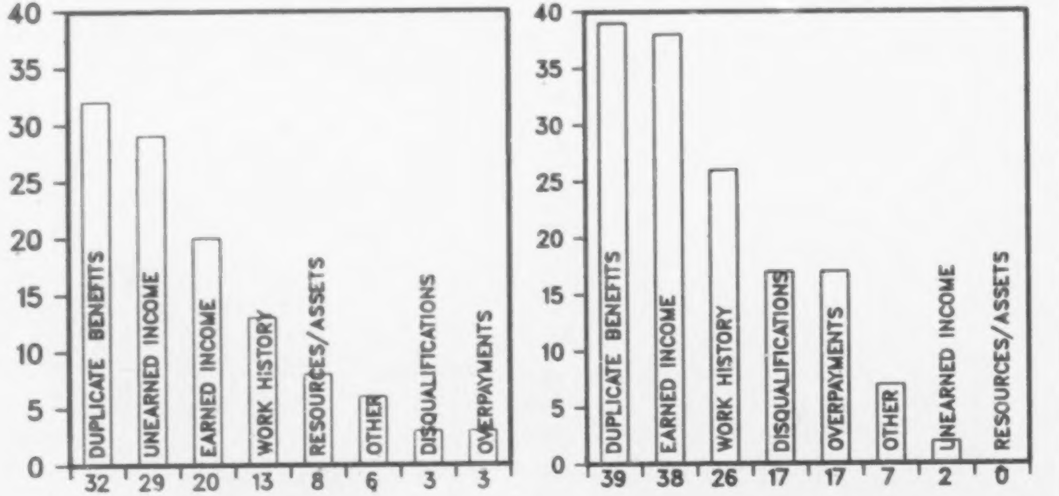
* The number of techniques listed in the graph is greater than the number of techniques reported because many techniques had multiple goals.

NUMBER OF TECHNIQUES VERIFYING ELIGIBILITY FACTORS, BY PROGRAM *



* The number of techniques listed for each graph is greater than the number of techniques reported for each program because many techniques had multiple goals.

NUMBER OF TECHNIQUES VERIFYING ELIGIBILITY FACTORS, BY PROGRAM *



MEDICAID

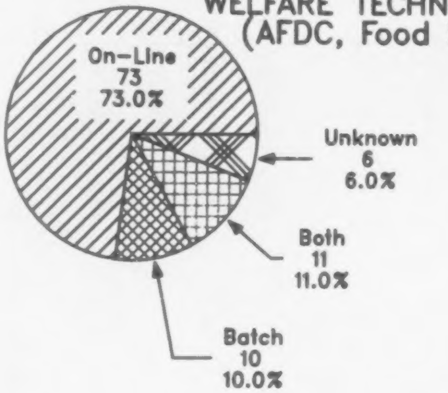
UNEMPLOYMENT INSURANCE

* The number of techniques listed for each graph is greater than the number of techniques reported for each program because many techniques had multiple goals.

METHOD OF COMPUTER PROCESSING

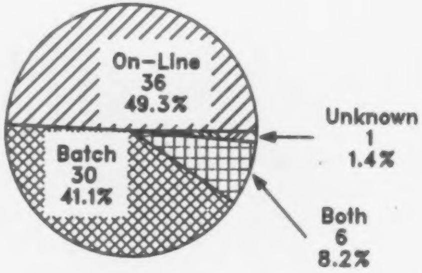
WELFARE TECHNIQUES
(AFDC, Food Stamps and Medicaid)

Total Number of Welfare Techniques Reported = 100 (58% of the total 173 techniques reported)



EMPLOYMENT SECURITY TECHNIQUES
(Unemployment Insurance)

Total Number of Employment Security Techniques Reported = 73 (42% of the total 173 techniques reported)



INDEX OF TECHNIQUES BY PROGRAM, FACTOR VERIFIED AND PAGE NUMBER

The techniques listed under each program verify an eligibility element for the program indicated. It should be noted that the technique may verify eligibility for multiple programs. The listing below indicates only one program so readers may see the universe of techniques for each program.

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
AL - Verification of Lack of SSI Income			X						42
AL - Verification of AFDC Reported Income as Compared to Food Stamp Reported Income			X						43
AL - Verification of Applicant Not Already Receiving AFDC	X								41
AL - Verification of WIN Registration								X	44
AK - Eligibility Information System	X	X	X						48
AZ - CASIS Inquiry & APIS System	X								50
AZ - Ul/Base Wage Verification through On-Line Inquiry		X	X	X					51
AZ - DMV Check					X				52
AR - ESD On-Line		X	X	X					55

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
CA - File Compatibility Check	X								57
CO - Interdepartmental Exchange		X	X						60
CO - State Data Exchange			X						61
CT - Prior Eligibility	X								65
CT - Labor Access		X	X	X					66
DE - Duplicate Benefit Check	X								68
DE - Client Wage & UCB Check		X	X						69
DE - Previous Client Income & Resource Check		X	X		X				70
DE - SDX Interface			X						71
DE - Verification of Client Information Throughout AFDC, Food Stamp and Medicaid Eligibility Processing			X		X				72
DE - Verification of Client Ineligibility						X			73
DE - Verification of Overpayment Status							X		74
DE - Child Protective Services Check								X	75

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
DC - On-Line Wage & UIB Clearance Check		X	X						77
DC - Project Checkmate		X	X		X				78
DC - On-Line Motor Vehicle Records					X			X	79
DC - On-Line School Attendance								X	80
DC - Operator Permit Records								X	81
FL - Duplicate Benefits Check	X								85
GA - Duplicate Benefits Check	X								88
HA - Duplicate Benefits Check	X								91
HA - UCB Check			X						92
HA - DMV Match					X				93
HA - Persons Previously Overpaid							X		95
ID - Prior Contact Check	X					X	X		96
IL - Applicant Verification	X	X	X	X					100
IN - DPW 95/SSN Cross Match		X	X	X					104
IA - State Identification System	X								109

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
IA - Automated Benefit Calculation System Screens	X								110
IA - State Data Exchange			X						111
KY - Screening for Duplicate SSNs	X								115
LA - CLIENT	X								117
ME - Automatic Checks/Edits Duplicate Records	X								119
ME - Worker Generated Computerized Request - Wage, UI Records		X	X	X					120
ME - Worker Generated Computerized Request - Motor Vehicle Records					X				121
MD - Wage Match		X	X	X					123
MD - AMF Screening	X								124
MI - Client Information System Duplicate Benefits Check	X								125
MI - DSS/Secretary of State Terminal Project					X				127

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
MS - MAVERICS	X	X	X	X	X			X	130
MO - Employment Security Wage/UCB Match		X	X	X					134
MO - Birth Records Match								X	135
NV - Welfare Referral System Income Assistance Check	X								140
NV - AFDC, Food Stamps, & Medicaid/Applicant Wage Match		X	X	X					141
NV - Welfare Referral System Wage & UCB Match		X	X						142
NH - Automated Eligibility Management Systems	X								144
NH - Prescreen for Wage & UCB	X	X	X						145
NJ - UIB Verification System			X						147
NM - 198C	X								150
NY - Resource File Integration		X		X					154
NY - Overnight Clearance System		X		X					155
NC - Name Search for EIS	X								158

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
NC - Employment Security Commission File		X	X	X					160
NC - State Data Exchange			X						161
NC - DMV Match					X				163
NC - SSA Query Card			X						162
ND - TECS	X				X				165
OK - ALFX Look-Up	X		X						168
OK - Case Number Assignment	X								169
OR - Central Client Index	X		X						170
OR - Employment Division Inquiry		X	X						172
OR - CASCADE	X	X	X	X					173
PA - Wage/UC Inquiry System		X	X	X					174
TN - Clearinghouse	X	X	X	X				X	181
TX - NOA Report	X								183
TX - Automated Perfect Match of Client Biographical Information	X								184
TX - OTIS	X								185

AFDC PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
TX - Eligibility Worker Requested Wage/UCB Match		X	X	X					186
TX - SSA Query Card System			X						187
VT - Name & SSN Match	X								195
VT - UCB Match			X						196
WA - File Clearance & Pre-authorization Cross Checks	X								202
WA - COSMOS Clearance Process	X					X	X	X	203
WI - Match the Applicant's SSN Against SSN of Active Caseheads	X								205
WV - Client Index System	X								212
TOTALS:	38	26	38	17	11	3	4	9	

FOOD STAMP PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
AK - Eligibility Information System	X	X	X						48
AZ - CASIS Inquiry & APIS System	X								50
AZ - UI/Base Wage Verification through On-Line Inquiry		X	X	X					51
AZ - DMV Check					X				52
AR - Screening of Head of Households SSN	X								54
AR - ESD On-Line		X	X	X					55
CA - File Compatibility Check	X								57
CO - Dual Participation Check on Head of Household	X								59
CO - Interdepartmental Exchange		X	X						60
CO - State Data Exchange			X						61
CT - Prior Eligibility	X								65
CT - Labor Access		X	X	X					66
DE - Duplicate Benefit Check	X								68
DE - Client Wage & UCB Check		X	X						69

FOOD STAMP PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
DE - Previous Client Income & Resource Check		X	X		X				70
DE - SDX Interface			X						71
DE - Verification of Client Information Throughout AFDC, Food Stamp, and Medicaid Eligibility Processing			X		X				72
DE - Verification of Client Ineligibility Periods						X			73
DE - Verification of Overpayment Status							X		74
DE - Child Protective Services Check									75
DC - On-Line Wage & UIB Clearance Check		X	X						77
DC - On-Line Motor Vehicle Records					X			X	79
DC - On-Line School Attendance Records								X	80
DC - Operator Permit Records								X	81
FL - Duplicate Benefits Check via SSN	X								84

FOOD STAMPS PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
GA - Duplicate Benefits Check	X								88
HA - Duplicate Benefits Check	X								91
HA - UCB Check			X						92
HA - DMV Match					X				93
HA - Persons Disqualified						X			94
HA - Persons Previously Overpaid							X		95
ID - Prior Contact Check	X					X	X		96
ID - State Data Exchange			X						97
ID - Persons Disqualified from Food Stamp Program due to IPV						X			98
IL - Applicant Verification	X	X	X	X					100
IN - DPW 95/SSN Cross Match		X	X	X					104
IA - State Identification System	X								109
IA - Automated Benefit Calculation System Screens	X								110

FOOD STAMPS PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
IA - State Data Exchange			X						111
IA - Intentional Program Violation Disqualification						X			112
KY - Disqualification File/ Duplicate Participation Check	X					X			116
LA - CLIENT	X								117
ME - Automatic Checks/Edits - Duplicate Records	X								119
ME - Worker Generated Computerized Request - Wage, UI Records		X	X	X					120
ME - Worker Generated Computerized Request - Motor Vehicle Records					X				121
MD - Wage Match		X	X	X					123
MD - AMF Screenings	X								124
MI - Client Information System Duplicate Benefits Check	X								125
MI - DSS/Secretary of State Terminal Project					X				127

FOOD STAMPS PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
MS - MAVERICS	X	X	X	X	X			X	130
MO - Employment Security Wage/UCB Match		X	X	X					134
NV - Welfare Referral System Income Assistance Check	X								140
NV- AFDC, Food Stamps & Medicaid Applicant Match		X	X	X					141
NV - Welfare Referral System Wage & UCB Match		X	X						142
NH - Automated Eligibility Management Systems	X								144
NH - Prescreen for Wage & UCB	X	X	X						145
NJ - UIB Verification System			X						147
NM - Duplicate Benefits Check	X								151
NM - HPDX			X						152
NM - HPWX			X	X				X	153
NY - Resource File Integration		X		X					154

FOOD STAMPS PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
NY - Overnight Clearance System		X		X					155
NC - Screen Comparison for Duplicate Participation	X								159
NC - Employment Security Commission File		X	X	X					160
NC - State Data Exchange			X						161
NC - DMV Match					X				163
NC - SSA Query Card System			X						162
ND - TECS	X				X				165
OK - ALFX Look-Up	X		X						168
OK - Case Number Assignment	X								169
OR - Verification of Eligibility	X								171
OR - CASCADE	X	X	X	X					173
PA - Wage/UC Inquiry System		X	X	X					174
SC - Employment Security Commission/Food Stamp Match & Unduplicated Participation	X	X	X	X					179

FOOD STAMPS PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
TN - Clearinghouse	X	X	X	X				X	181
TX - NOA Report	X								183
TX - Automated Perfect Match of Client Biographical Info	X								184
TX - OTIS	X								185
TX - Eligibility Worker Requested Wage/UCB Match		X	X	X					186
TX - SSA Query Card System			X						187
VT - Name & SSN Match	X								195
VT - UCB Match			X						196
WA - File Clearance & Preauthorization Cross Checks	X								202
WA - COSMOS	X					X	X	X	203
WI - Match the Applicant's SSN Against the SSN of Active Caseheads	X								205
WV - Client Index System	X								212
TOTALS:	40	25	38	19	10	7	4	8	

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
AL - Automated Application System	X								45
AK - Eligibility Information System	X	X	X						48
AZ - CASIS Inquiry & APIS System	X								50
AZ - DMV Check					X				52
AR - ESD On-Line		X	X	X					55
CA - File Compatiblity Check	X								57
CO - Interdepartmental Exchange		X	X						60
CO - State Data Exchange			X						61
CT - Prior Eligibility	X								65
CT - Labor Access		X	X	X					66
DE - Duplicate Benefit Check	X								68
DE - Client Wage & UCB Check		X	X						69
DE - Previous Client Income & Resource Check		X	X		X				70
DE - SDX Interface			X						71

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
DE - Verification of Client Information Throughout AFDC, Food Stamp, and Processing			X		X				72
DE - Verification of Client Ineligibility Periods						X			73
DE - Third Party Medical Insurance Verification								X	76
DE - Child Protect Service Check									75
DC - On-Line Wage & Clearance Check		X	X						77
DC - On-Line Motor Vehicle Records					X			X	79
DC - On-Line School Attendance Records								X	80
DC - Operator Permit Records								X	81
GA - Duplicate Benefits Check	X								88
HA - Duplicate Benefits Check	X								91
HA - UCB Check			X						92
HA - DMV Match					X				93

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
HA - Persons Previously Overpaid							X		95
ID - Prior Contact Check	X					X	X		96
ID - State Data Exchange			X						97
IL - Applicant Verification	X	X	X	X					100
IN - DPW 95/SSN Cross Match		X	X	X					104
IA - State Identification System	X								109
IA - Automated Benefit Calculation System Screens	X								110
IA - State Data Exchange			X						111
KY - Screening for Duplicate SSNs	X								115
LA - CLIENT	X								117
ME - Worker Generated Computerized Request - Wage, UI Records		X	X	X					120
ME - Automatic Checks/Edits - Duplicate Records	X								119

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
ME - Worker Generated Computerized Request - Motor Vehicle Records					X				121
MD - AMF Screening	X								124
MI - Client Information System Duplicate Benefits Check	X								125
MI - DSS/Secretary of State Terminal Project					X				127
MO - Employment Security Wage/UCB Match		X	X	X					134
MO - Birth Records Match								X	135
NV - AFDC, Food Stamps & Medicaid Applicant Wage Match		X	X	X					141
NV - Welfare Referral System Wage & UCB Match		X	X						142
NH - Automated Eligibility Management System	X								144
NY - Resource File Integration		X		X					154
NY - Overnight Clearance System		X		X					155

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
NC - Name Search for EIS	X								158
NC - Employment Security Commission File		X	X	X					160
NC - State Data Exchange			X						161
NC - DMV Match					X				163
NC - SSA Query Card System			X						162
OK - ALFX Look-Up	X		X						168
OK - Case Number Assignment	X								169
OR - Central Client Index	X								170
OR - Employment Division Inquiry		X	X						172
OR - CASCADE	X	X	X	X					173
PA - Wage/UC Inquiry System		X	X	X					174
TN - Clearinghouse	X	X	X	X					181
TX - BOA Report	X								183
TX - Automated Perfect Match of Client Biographical Info	X								184
TX - OTIS	X								185

MEDICAID PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
TX - SSA - Query Card System			X						187
VT - Name & SSN Match	X								195
VT - UCB Match			X						196
WA - File Clearance & Preauthorization Cross Checks	X								202
WA - COSMOS	X					X	X		203
WI - Match the Applicant's SSN Against the SSN of Active Caseheads	X								205
WV - Client Index System	X								212
TOTALS:	32	20	29	13	8	3	3	6	

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
AL - Monetary Eligibility for UCB		X		X					46
AL - Nonmonetary Eligibility for UCB						X			47
AK - Pseudo Monetary	X	X		X					49
AZ - Initial Claim Processing	X	X							53
AR - Crossmatch - Wage File, Previous Claim File	X	X				X			56
CA - Use of Computer Files of Employer Wages & Eligibility Flags	X	X				X	X		58
CO - Establishment of Monetary Eligibility by Wage Data Input		X							62
CO - Alien Status Check								X	63
CO - Illegal Alien SSN Check								X	64
CT - Claimant Name/Wage Record Match	X	X		X					67
DC - Claim Check	X	X							82

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
DC - Monetary Determination		X		X					83
FL - Previous Valid Claim	X								86
FL - Fraud Stop Orders & Labor Dispute Stop Orders						X			87
GA - Entry of Initial UI Claim	X	X							89
GA - Preliminary Monetary Determination		X		X					90
ID - BASIS	X	X		X		X	X		99
IL - Duplicate Claim Checking	X								101
IL - Claimant Dependency	X								102
IL - Determine Monetary Eligibility		X		X					103
IN - Duplicate Benefits Check	X								105
IN - Monetary Determination		X							107
IN - Dependency Check								X	108
IN - Initial Claim	X								106

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
IA - UI Claim	X	X		X					113
KS - Monetary Pre-Determination		X		X					114
LA - Processing of Separation Notices						X			118
ME - UI Initial Claim Process	X	X		X				X	122
MA - Initial Claim Verification	X						X	X	125
MI - Claimant Status Verification	X					X	X		128
MI - Employer Liability Verification								X	129
MS - Monetary Eligibility For UCB	X	X		X					131
MS - Nonmonetary Eligibility for UCB						X			132
MS - Use of Computer File to Detect Overpayments							X		133
MO - Premonetary Determination Process		X		X					136

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
MO - Initial & Continued Claims Process						X			137
MO - Overpayments Check							X		138
MT - Name Verification	X	X							139
NV - Pre-Monetary Determination	X	X		X					143
NH - Monetary Determinations	X	X		X		X	X		146
NJ - LOOPS	X		X				X		148
NJ - Initial Claims Check		X		X					149
NY - Original Claim Preliminary Verification	X								156
NY - Verification of Eligibility to Establish a Valid Original Claim		X		X		X			157
NC - Monetary Determination		X							164
ND - No Name	X	X		X					166
OH - Initial Claim Verification	X							X	167
PA - Financial Determination	X	X		X					175

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disquali- fications	Over- payments	Other	Page Number
PA - Prevention of Payment Where An Overpayment Balance Exists							X		176
PR - No Name	X	X		X					177
RI - Claims Control	X		X				X		178
SC - Monetary Determination Process	X	X		X			X		180
TN - Pre-eligibility Check	X	X		X			X		182
TX - Initial Claims Process	X								188
TX - Premonetary Determination		X							189
TX - Monetary Determination Process		X							190
TX - Initial & Weekly Claims Process						X			191
TX - Overpayment Absorption Process						X			192
UT - Cross-Match	X					X	X		193
UT - Premonetary Determination		X		X					194

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Overpayments	Other	Page Number
VT - New Claims Process	X								197
VA - Duplicate Claim Verification	X								198
VA - Name Check Verification		X		X					199
VA - Disqualification or Overpayment Verification						X	X		200
VI - Initial Claim Determination	X	X							201
WA - Monetary Determination Process	X	X		X		X			204
WI - SSN Check	X								206
WI - Disqualification & Overpayment Check						X	X		207
WY - Initial Claims Process	X								208
WY - UI Monetary Eligibility		X		X					209
WY - Initial and Weekly Claims Process						X			210

UNEMPLOYMENT INSURANCE PROGRAM

Name of Technique	Duplicate Benefits	Earned Income	Unearned Income	Work History	Resources/ Assets	Disqualifications	Over-payments	Other	Page Number
WY - Overpayment Absorption Process							X		211
WV - Eligibility for UI	X	X		X					213
TOTALS:	39	38	2	26	0	17	17	7	

OMB # 0990-0127
Exp. date 12/31/84

APPENDIX A

SURVEY OF COMPUTERIZED FRONT-END VERIFICATION TECHNIQUES
STATE OR LOCAL FRONT-END TECHNIQUE PROFILE

Please indicate your answers below. If your State has more than one automated front-end eligibility verification technique in place or under development, please reproduce the questionnaire and complete one copy for each technique. If the technique is under development, do not answer questions 13, 16, and 19. For your information, a computerized front-end eligibility verification technique means any automated or computerized technique which is used to aid in determining the eligibility of applicants prior to the payment of any benefits.

1) Name of agency using technique ____________________

Name of State ____________________

2) Name of front-end verification technique ____________________

____

3) Describe the technique and its goals in nontechnical terms. Include a step-by-step description of the workflow. (Do not include a flowchart of the actual computer program).

4) Is the computerized technique

_____ a match? (A match is the comparison of data elements on two or more computer files.)
_____ a screen? (A screen is the comparison or analysis of data elements on one computer file.)
_____ an edit? (An edit is a check in the system to assure that data elements entered are within certain limits.)
_____ other? (Specify)

5) Check all specific eligibility-related factor(s) on which the computerized technique provides information.

Duplicate Benefits _____
Identity _____
Income _____
Resources/Assets _____
Social Security Number _____
Work History _____
Work Registration _____
Other(s) (Specify: e.g., household composition, residency)
__________________ _____
__________________ _____

6) Check all program(s) involved in the computerized technique:

AFDC ____
Food Stamps
  Public Assistance ____
  Non-Public Assistance ____
Medicaid ____
Unemployment Insurance ____
Other (Specify) ____
____

7) What files are used in the computerized technique? (e.g., in the case of a match, AFDC applicant files might be matched against State birth records).

8) Is the technique

(a) _____ under development?
If so, when was it begun? __________________________
What is the estimated completion date? ______________
____

(b) _____ operational?
How long has it been operating?
____
____

9) Is the technique part of a demonstration or pilot project?

Yes_____ No_______

If so, which Federal agency is sponsoring the project?

10) Is the technique used statewide?

Yes _____ No _____

If No:
In which jurisdictions is it used?

Why isn't the technique used statewide?

If statewide use is anticipated, when will it occur?

11) How does management track the disposition of hits? (A hit is defined as a matching of two or more data elements with different or inconsistent information).

12) What were the approximate developmental costs of the computerized technique? (Some of the categories to consider include hardware/software, personnel, computer processing time, file conversion, overhead, and staff training).

13) What are the approximate annual operating costs associated with the use of the computerized technique? (Consider costs for hardware, software, personnel, and so on).

14) Indicate by a checkmark below the sources of funding for the computerized technique.

	Developmental Funding	Operational Funding
Local	____________	____________
State	____________	____________
Federal	____________	____________
Other	____________	____________

If Federal or "other" funding is checked, list the Federal agency or other source and indicate whether funding was for development or for operation of the technique.

15) What are the approximate annual savings derived or projected from the use of the technique? How are these savings computed?

16) As a result of the use of the technique,
What is the estimated annual number of applications denied?
____
What is the estimated annual number of raw hits? (A raw hit is an unvalidated or unverified hit). ____________________
What percentage of the raw hits were valid hits? (That is, hits that were validated as exceptions.) ____________________

17) Do you require that applicants be notified in advance of the use of the computerized technique?

Yes______ No_____

If so, is advance notice required by State law?

Yes______ No_____

What method of notification is used?

18) What provisions are made for preventing the unauthorized disclosure of information?

19) Has legal action been brought against the State due to the employment of the technique?

Yes_____ No_____

20) Are there any limitations on sharing the technique with Federal, State or local jurisdictions? If so, please specify.

21) List below the person who may be contacted by State and Federal officials for further information.

Name of contact person ______________________

Title/Position ______________________

Address ______________________

____

____

Phone number ( ) __________ __________

Date survey completed ______________________

If you have any questions about this form, please contact:

Elisabeth Handley
Project Leader
HHS, Office of Inspector General
Room 5643 North Building
330 Independence Avenue, S.W.
Washington, D.C. 20201
(202) 472-5270 or
(202) 472-3480

APPENDIX B

GLOSSARY OF ABBREVIATIONS AND TERMS

- AFDC - Aid to Families with Dependent Children Program. A State- and federally-administered program which provides financial aid to needy children and their caretaker relatives.

- BENDEX - Beneficiary and Earnings Data Exchange. An automated system SSA uses to provide States with the eligibility status and payment information of recipients of Social Security Retirement, Survivors and Disability Insurance and eligibility status only of recipients of Supplemental Security Income, Medicare, Black Lung and Railroad Retirement benefits.

- DoB - Date of Birth

- Edit - a check in the system to assure that data elements entered are within certain limits.

- ETA - Employment and Training Administration, U.S. Department of Labor

- Eligibility Determination - the entire process of determining an applicant's eligibility, including the verification of eligibility factors and the calculation of benefit levels.

- Eligibility Verification - the process of confirming the accuracy of reported eligibility factors such as earned income, SSN, etc.

- Front-end - prior to the payment of any benefits or awards to benefit program applicants.

- FNS - Food and Nutrition Service, U.S. Department of Agriculture

- FS - Food Stamp Program. A State- and federally-administered benefit program which provides food coupons to low-income households to augment their food budget.

- HCFA - Health Care Financing Administration, U.S. Department of Health and Human Services

- Match - the comparison of data elements on two or more computer files (compare to "Screen").

- MCD - Medicaid Program. A State- and federally-administered program which provides medical assistance to welfare recipients and other medically needy persons.
- OFA - Office of Family Assistance, Social Security Administration, U.S. Department of Health and Human Services
- Prepayment - See front-end
- Real Time - near-instantaneous response to on-line inquiries from a computer terminal.
- Sanction - a punishment or penalty such as a fine or exclusion from participation.
- Screen - the comparison of analysis of data elements on one computer file (compare to "Match").
- SDX - State Data Exchange. An SSA automated interface system which lists recipients and payment amounts for Supplemental Security Income.
- SSA - Social Security Administration, U.S. Department of Health and Human Services.
- SSN - Social Security Number
- UCB - Unemployment Compensation Benefits (used interchangeably with "UI")
- UI - Unemployment Insurance Program (used interchangeably with "UCB"). A State- and federally-administered program which provides cash unemployment compensation to those temporarily out of work.
- WIN - Work Incentive Program

GAO QUESTIONNAIRE ANNOTATED TO
SHOW RESPONSES OF REPLYING STATES

U.S. GENERAL ACCOUNTING OFFICE
SURVEY OF STATE IMPLEMENTATION OF THE INCOME AND ELIGIBILITY PROVISIONS OF THE 1984 DEFICIT REDUCTION ACT

/ /

INTRODUCTION

The U.S. General Accounting Office, an agency of the U.S. Congress, is conducting a survey of the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as part of an effort to monitor federal and state efforts to implement the income and eligibility provisions of section 2651 of the Deficit Reduction Act of 1984 (DEFRA).

In this questionnaire we are asking the states to share their views on various DEFRA provisions; provide information about the status of their income and eligibility verification system (IEVS) development; and indicate how they plan to implement the DEFRA requirements within the required timeframes.

Please complete and return this questionnaire within two weeks, if possible. The questions can be answered by checking a box or writing in a number or a few words. We realize that some of the response choices we ask you to select from may not exactly fit the situation in your state. In this event, please select the response that most closely describes your situation.

A self-addressed, business reply envelope is enclosed for your convenience. If you have any questions, call Dick Halter or Dave Pasquarello at 215/597-4330. They will be happy to help you. Should the return envelope be misplaced, mail the completed questionnaire to:

U.S. General Accounting Office
Dave Pasquarello
434 Walnut St., 11th floor
Philadelphia, PA 19106-3797

Thank you for your assistance.

Official responsible for IEVS implementation in your state:

Name: ______________________

Title: ______________________

Agency: ______________________

Official responsible for filling out this questionnaire:

Name: ______________________

Title: ______________________

Agency: ______________________

Phone number: ______________________

Has the official responsible for filling out this questionnaire had experience working in any of the programs listed below? (CHECK ALL THAT APPLY.)

1.[48]Aid to Families with Dependent Children (AFDC)

2.[45]Food stamps

3.[41]Medicaid

4.[3]Unemployment Compensation

5.[20]Other (SPECIFY.)

____

____

I. OVERALL AUTOMATED SYSTEM DEVELOPMENT

The 1984 DEFRA requires each state to operate an income and eligibility verification system (IEVS) that would handle data exchanges within and between states, and receive and use tax data from both the Internal Revenue Service (IRS) and the Social Security Administration (SSA). Questions in this section refer to the system your state will be using to implement the DEFRA requirements.

1. Which of the statements below best describes how your state intends to meet DEFRA requirements. (CHECK ONE.)

   1.[6]Existing system already meets IEVS requirements or will meet all requirements with minimum modifications within the required timeframes. This system, with the necessary modifications, if any, will be the state's operational system for the foreseeable future.
   --►(SKIP TO QUESTION 8.)

   2.[12]A system currently planned or under development will meet or will be modified to meet the requirements within the required timeframes. This system will replace the existing system and become the state's operational system for the foreseeable future.
   --►(SKIP TO QUESTION 8.)

   3.[32]A system currently planned or under development will meet or will be modified to meet the requirements and will ultimately become the state's operational system for the future. However, this system cannot be implemented within the required timeframes. Therefore, the state will meet the requirements by an interim modification of an existing system, or implementation or a temporary solution to meet requirements.

2. Currently, at what stage of development is this ultimate automated system? (CHECK ONE.)

   1.[2]Fully developed but not yet fully operational

   2.[19]Development in process

   3.[11]Planning for development

3. How long after 10/1/86 do you estimate your state's ultimate system will be fully operational? (CHECK ONE.)

   1.[3]within less than 3 months

   2.[1]in 3 to less than 6 months

   3.[3]in 6 to less than 9 months

   4.[4]in 9 to less than 12 months

   5.[21]in 12 months or more

4. In your estimation, how efficiently will your state be able to meet IEVS requirements from 10/1/86 until your ultimate system becomes fully operational? (CHECK ONE.)

   1.[0]very efficiently

   2.[13]efficiently

   3.[19]inefficiently

5. Will resources need to be diverted from development of your ultimate system to modify an existing system, or to implement a temporary solution, to meet DEFRA requirements? (CHECK ONE.)

   1.[24]Yes

   2.[8]No--►(SKIP TO QUESTION 8.)

6. To what extent, if any, will this diversion of resources from the development of your jurisdiction's ultimate system contribute to a delay in its eventual implementation? (CHECK ONE.)

1. [1] To a very great extent
2. [6] To a great extent
3. [11] To a moderate extent
4. [5] To some extent
5. [2] To little or no extent -->(SKIP TO QUESTION 8.)

7. If your jurisdiction did not have to take the measure of modifying an existing system, or implementing a temporary solution, solely to meet the 10/1/86 deadline, how much earlier do you estimate your jurisdiction would be able to implement its ultimate system? (CHECK ONE.)

1. [6] less than 1 month earlier
2. [2] from 1 to less than 3 months earlier
3. [3] from 3 to less than 6 months earlier
4. [5] from 6 to less than 9 months earlier
5. [3] from 9 to less than 12 months earlier
6. [2] 12 months earlier or more

8. Beyond your current programming budget, will your jurisdiction need additional funds to implement the DEFRA requirements within the required timeframe?

1. [30] Yes
2. [15] No-->(SKIP TO QUESTION 11.)

9. Indicate whether or not you plan to obtain any of the needed funds from each of the sources listed below. (CHECK ONE BOX FOR EACH SOURCE.)

	YES	NO
	1	2
1. Federal funding	30	5
2. State funding	24	12
3. Reprogram funds from other programs	10	26
4. Other (SPECIFY.) ______ ______	4	32

10. Can these additional funds be obtained by 10/1/86? (CHECK ONE.)

1. [5] Definitely yes
2. [15] Probably yes
3. [11] Probably no
4. [5] Definitely no

I. INCOME AND ELIGIBILITY VERIFICATION SYSTEM PROFILE

1. In SECTION A enter the number of the statement below that best describes how your jurisdiction met each DEFRA requirement as of 5/29/86.

   1. The 5/29/86 deadline was waived by a federal agency until 10/1/86.
   2. The requirement was met as of 5/29/86 using an interim or temporary system. Another system is planned or under development that will ultimately become the jurisdiction's operational system for the foreseeable future.
   3. The requirement was met as of 5/29/86 using the jurisdiction's existing system (with minimal, if any, modifications). This same system will be the jurisdiction's operation system for the foreseeable future.
   4. The requirement was met as of 5/29/86 using a newly developed system (whether or not it was based on an existing system). This same system will be the jurisdiction's operational system for the foreseeable future.

   For each requirement for which your response in SECTION A is either statement "1" or "2", in SECTION B enter the number of the statement below that best describes how your jurisdiction plans to fulfill each DEFRA requirement as of 10/1/86.

   1. As of 10/1/86 the requirement will be met using an interim or temporary system. Another system is planned or under development that will ultimately become the jurisdiction's operational system in the foreseeable future.
   2. As of 10/1/86 the requirement will be met using a system that will be the jurisdiction's ultimate operational system for the foreseeable future.

   In SECTION C indicate whether, currently, each provision is fully, partially, or not yet implemented in your jurisdiction. (CHECK ONE BOX FOR EACH PROVISION.)

   In SECTION D indicate whether your jurisdiction believes the cost (in terms of start up and operation dollars, time and human effort) expended to implement each provision is worth the potential benefit (in terms of program dollars saved.) (CHECK ONE BOX FOR EACH PROVISION. DO NOT RESPOND IN SHADED BOXES.)

	SECTION A HOW JURISDICTION MET RE-QUIREMENT AS OF 5/29/86?	SECTION B HOW JURISDICTION WILL MEET REQUIREMENT AS OF 10/1/86?	SECTION C CURRENT IMPLEMENTATION?			SECTION D COST VS. BENEFIT?		
			FULL	PAR-TIAL	NONE	COST EXCEEDS BENEFIT	COST EQUALS BENEFIT	BENEFIT EXCEEDS COST
			1	2	3	4	5	6
1. Use standard record formats	1-35 2-8 3-5 4-2	1 - 27 2 - 16	6	23	20	16	17	10
2. Obtain and verify program applicants' and family members' SSN	1-30 2-8 3-13 4-0	1 - 24 2 - 14	18	28	5	5	19	20
3. Validate program applicants'/recipients' SSN with SSA Third Party Query, Bendex, or Enumeration/validation system	1-33 2-9 3-9 4-0	1 - 24 2 - 18	9	37	5	7	18	18
4. Obtain and use state wage data for income/eligibility verification	1-19 2-10 3-15 4-0	1 - 20 2 - 9	17	27	0	10	5	24

In SECTION A enter the number of the statement below that best describes how your state met each DEFRA requirement as of 5/29/86.

1. The 5/29/86 deadline was waived by a federal agency until 10/1/86.
2. The requirement was met as of 5/29/86 using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system for the foreseeable future.
3. The requirement was met as of 5/29/86 using the state's existing system (with minimal, if any, modifications). This same system will be the state's operational system for the foreseeable future.
4. The requirement was met as of 5/29/86 using a newly developed system (whether or not it was based on an existing state system). This same system will be the state's operational system for the foreseeable future.

For each requirement for which your response in SECTION A is either statement "1" or "2", in SECTION B enter the number of the statement below that best describes how your state plans to fulfill each DEFRA requirement as of 10/1/86.

1. As of 10/1/86 the requirement will be met using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system in the foreseeable future.
2. As of 10/1/86 the requirement will be met using a system that will be the state's ultimate operational system for the foreseeable future.

In SECTION C indicate whether, currently, each provision is fully, partially, or not yet implemented in your state. (CHECK ONE BOX FOR EACH PROVISION.)

In SECTION D indicate whether your state believes the cost (in terms of start up and operation dollars, time and human effort) expended to implement each provision is worth the potential benefit (in terms of program dollars saved.) (CHECK ONE BOX FOR EACH PROVISION. DO NOT RESPOND IN SHADED BOXES.)

	SECTION A HOW STATE MET REQUIREMENT AS OF 5/29/86?	SECTION B HOW STATE WILL MEET REQUIREMENT AS OF 10/1/86?	SECTION C CURRENT IMPLEMENTATION?			SECTION D COST VS. BENEFIT?		
			FULL 1	PARTIAL 2	NONE 3	COST EXCEEDS BENEFIT 4	COST EQUALS BENEFIT 5	BENEFIT EXCEEDS COST 6
5. Exchange data between needs-based programs within your state	1 - 20 2 - 13 3 - 17 4 - 0	1 - 27 2 - 6	24	24	3	9	8	29
6. Exchange wage and needs-based program data with other states	1 - 27 2 - 11 3 - 5 4 - 1	1 - 26 2 - 12	2	21	21	22	12	7
7. Obtain and use IRS tax data for income/eligibility verification	1 - 50 2 - 0 3 - 0 4 - 0	1 - 30 2 - 20	0	8	43	29	9	5
8. Obtain and use SSA tax (wage, private pension & self-employment) data for income/eligibility verification	1 - 42 2 - 6 3 - 2 4 - 0	1 - 32 2 - 16	2	22	27	33	6	6

In SECTION A enter the number of the statement below that best describes how your state met each DEFRA requirement as of 5/29/86.

1. The 5/29/86 deadline was waived by a federal agency until 10/1/86.
2. The requirement was met as of 5/29/86 using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system for the foreseeable future.
3. The requirement was met as of 5/29/86 using the state's existing system (with minimal, if any, modifications). This same system will be the state's operational system for the foreseeable future.
4. The requirement was met as of 5/29/86 using a newly developed system (whether or not it was based on an existing state system). This same system will be the state's operational system for the foreseeable future.

For each requirement for which your response in SECTION A is either statement "1" or "2", in SECTION B enter the number of the statement below that best describes how your state plans to fulfill each DEFRA requirement as of 10/1/86.

1. As of 10/1/86 the requirement will be met using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system in the foreseeable future.
2. As of 10/1/86 the requirement will be met using a system that will be the state's ultimate operational system for the foreseeable future.

In SECTION C indicate whether, currently, each provision is fully, partially, or not yet implemented in your state. (CHECK ONE BOX FOR EACH PROVISION.)

In SECTION D indicate whether your state believes the cost (in terms of start up and operation dollars, time and human effort) expended to implement each provision is worth the potential benefit (in terms of program dollars saved.) (CHECK ONE BOX FOR EACH PROVISION. DO NOT RESPOND IN SHADED BOXES.)

	SECTION A HOW STATE MET RE-QUIREMENT AS OF 5/29/86?	SECTION B HOW STATE WILL MEET REQUIREMENT AS OF 10/1/86?	SECTION C CURRENT IMPLEMENTATION?			SECTION D COST VS. BENEFIT?		
			FULL	PAR-TIAL	NONE	COST EXCEEDS BENEFIT	COST EQUALS BENEFIT	BENEFIT EXCEEDS COST
			1	2	3	4	5	6
9. Safeguard IRS tax data	1-46 3-2 2-1 4-0	1 - 26 2 - 21	1	12	38			
10. Safeguard SSA tax data	1-35 3-9 2-6 4-0	1 - 25 2 - 16	12	16	23			
11. Safeguard your state's wage and needs-based program data	1-12 2-11 3-26 4-1	1 - 15 2-8	33	14	4			
12. Safeguard other states' wage and needs-based program data	1-19 2-12 3-17 4-0	1 - 18 2 - 13	21	17	10			

In SECTION A enter the number of the statement below that best describes how your state met each DEFRA requirement as of 5/29/86.

1. The 5/29/86 deadline was waived by a federal agency until 10/1/86.
2. The requirement was met as of 5/29/86 using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system for the foreseeable future.
3. The requirement was met as of 5/29/86 using the state's existing system (with minimal, if any, modifications). This same system will be the state's operational system for the foreseeable future.
4. The requirement was met as of 5/29/86 using a newly developed system (whether or not it was based on an existing state system). This same system will be the state's operational system for the foreseeable future.

For each requirement for which your response in SECTION A is either statement "1" or "2", in SECTION B enter the number of the statement below that best describes how your state plans to fulfill each DEFRA requirement as of 10/1/86.

1. As of 10/1/86 the requirement will be met using an interim or temporary system. Another system is planned or under development that will ultimately become the state's operational system in the foreseeable future.
2. As of 10/1/86 the requirement will be met using a system that will be the state's ultimate operational system for the foreseeable future.

In SECTION C indicate whether, currently, each provision is fully, partially, or not yet implemented in your state. (CHECK ONE BOX FOR EACH PROVISION.)

In SECTION D indicate whether your state believes the cost (in terms of start up and operation dollars, time and human effort) expended to implement each provision is worth the potential benefit (in terms of program dollars saved.) (CHECK ONE BOX FOR EACH PROVISION. DO NOT RESPOND IN SHADED BOXES.)

	SECTION A HOW STATE MET REQUIREMENT AS OF 5/29/86?	SECTION B HOW STATE WILL MEET REQUIREMENT AS OF 10/1/86?	SECTION C CURRENT IMPLEMENTATION?			SECTION D COST VS. BENEFIT?		
			FULL 1	PARTIAL 2	NONE 3	COST EXCEEDS BENEFIT 4	COST EQUALS BENEFIT 5	BENEFIT EXCEEDS COST 6
13. Take appropriate action on cases identified by IRS or SSA tax data within 10 days	1-49 2-1 3-0 4-0	1-28 2-22	0	11	40	33	6	6
14. Track record volume and report annually	1-48 3-1 2-1 4-0	1-29 2-20	0	15	35	29	12	4
15. Track case disposition and report annually	1-48 3-1 2-1 4-0	1-31 2-18	1	13	37	34	7	4

12. A coordinating agency or agencies will be needed in each state to handle data exchanges with the IRS Information Returns Processing (IRP) system and the SSA Bendex system. Please indicate how your state will be structured to accomplish this. (CHECK ONE.)

1. [47] a single agency will be responsible for coordinating your state's data exchanges with both SSA and IRS systems
2. [4] separate agencies will be responsible for coordinating your state's data exchanges with SSA and IRS systems

Questions 13 through 19 refer to the functions of this coordinating agency (or agencies if IRS and SSA data are each handled by a separate agency). Answer them in regard to how it (or they) will be functioning as of 10/1/86.

13. Indicate whether or not your state coordinating agency will screen IRS output files to eliminate cases in which data shows accurate income was reported by applicant/recipient.

1. [23] Yes--►(CONTINUE.)
2. [27] No---►(SKIP TO QUESTION 16.)

In questions 14 and 15 "case followup" refers to determination of differences between applicant/recipient-provided data and IEVS data through record comparisons; verification with applicant/recipient or third party where differences do exist; and case investigation and fraud referral where warranted.

14. Will your state coordinating agency perform IRS case followup independent of counties, user agencies, or caseworkers in your state?

1. [4] Yes--►(SKIP TO QUESTION 16.)
2. [18] No--►(CONTINUE.)

15. Indicate whether or not your state coordinating agency will be responsible for sorting and distributing IRS data files in each of the ways listed below. (CHECK ONE BOX FOR EACH ROW.)

	YES	NO
	1	2
1. Sort IRS output file by caseworker within each user agency and distribute subfiles to agencies for screening and case followup	28	18
2. Sort IRS output file by state user agency and distribute subfiles to each for screening and case followup	21	25
3. Sort IRS output file by county and distribute subfiles to each for screening and case followup	29	17

16. Indicate whether or not your state coordinating agency will screen SSA output files to eliminate cases in which data shows accurate income was reported by applicant/recipient.

1. [23] Yes--►(CONTINUE.)
2. [27] No---►(SKIP TO QUESTION 18.)

17. Will your state coordinating agency perform SSA case followup independent of counties, user agencies, or caseworkers in your state?

1. [4] Yes--►(SKIP TO QUESTION 19.)
2. [17] No---►(CONTINUE.)

18. Indicate whether or not your state coordinating agency will be responsible for sorting and distributing SSA data files in each of the ways listed below. (CHECK ONE BOX FOR EACH ROW.)

	YES	NO
	1	2
1. Sort SSA output file by caseworker within each user agency and distribute subfiles to agencies for screening and case followup	31	15
2. Sort SSA output file by state user agency and distribute subfiles to each for screening and case followup	25	21
3. Sort SSA output file by county and distribute subfiles to each for screening and case followup	29	17

III. USE OF SOCIAL SECURITY NUMBERS

19. Indicate whether or not your state currently requires applicants and family members to provide their social security numbers (SSNs) to each of the programs listed below. (CHECK ONE BOX FOR EACH PROGRAM.)

	STATE REQUIRES SSN FROM...		
	APPLICANTS ONLY	BOTH APPLICANTS AND FAMILY	NEITHER APPLICANTS NOR FAMILY
	1	2	3
1. Medicaid	6	42	2
2. Aid to Families with Dependent Children (AFDC)	3	41	2
3. Food Stamps	4	45	2

20. How does the cost (in terms of dollars, time, and human effort) of each of the following initiatives compare to its potential benefit (in terms of program dollars saved)? (CHECK ONE BOX FOR EACH ROW.)

	COST EXCEEDS BENEFIT	COST EQUALS BENEFIT	BENEFIT EXCEEDS COST
	1	2	3
1. Modify existing application forms to facilitate SSN verification	9	24	11
2. Case worker training to implement SSN verification	8	23	13

21. Which SSA system does your state most often use to validate a program recipient's SSN? (CHECK ONE.)

1. [3]Third party query system

2. [8]Bendex system

3. [38]Enumeration/validation system

22. About how long, on average, does it take SSA to answer your state's requests for SSN validation with the system your state most often uses? (CHECK ONE.)

1. [0]Less than 1 day

2. [1]1 day to less than 1 week

3. [0]1 week to less than 2 weeks

4. [5]2 weeks to less than 3 weeks

5. [7]3 weeks to less than 4 weeks

6. [32]4 weeks or more

7. [5]Can't determine--very little experience with SSA

23. In your opinion, how accurate are SSA's responses to your state's requests for SSN validation? (CHECK ONE.)

1. [9]very accurate (99-100%)

2. [31]accurate (95-98%)

3. [8]inaccurate (94% or less)

IV. STATE WAGE REPORTING

24. Is your state currently a wage reporting state?

1.[44]Yes→(SKIP TO QUESTION 31.)

2.[7]No

25. Which of the statements listed below best describes how your state will fulfill the DEFRA requirement to collect and record state wage data? (CHECK ONE.)

1.[4]adopt or create an entirely new system

2.[2]totally or almost totally redesign an existing state system

3.[1]make moderate changes to an existing state system

4.[0]make minimal changes to an existing state system

5.[0]use an existing state system essentially as it stands

26. Will this system also be used for unemployment compensation purposes?

1.[5]Yes

2.[2]No

27. Indicate whether your state believes the start up and operating costs to collect and record state wage data will exceed, equal, or fall short of the potential benefit (in terms of program dollars saved). (CHECK ONE.)

1.[2]cost exceeds benefit

2.[2]cost equals benefit

3.[2]cost falls short of benefit

28. Will this system require changes in your state's laws?

1.[6]Yes

2.[1]No

29. Will your state need special funding to start up and/or operate this sytem?

1.[7]Yes

2.[0]No

30. Will your state begin quarterly wage reporting by 9/30/88? (CHECK ONE.)

1.[5]Definintely yes

2.[2]Probably yes

3.[0]Probably not

4.[0]Definitely not

V. NEEDS-BASED AND WAGE DATA EXCHANGES WITHIN YOUR STATE

31. Listed below are the programs that must access and use state wage data. In each program, is this process currently automated or manual? (CHECK ONE BOX FOR EACH PROGRAM.)

	AUTOMATED --MOSTLY OFF-LINE 1	AUTOMATED --AS OFTEN OFF-LINE AS ON-LINE 2	AUTOMATED --MOSTLY ON-LINE 3	MANUAL 4	NOT APPLICABLE-- STATE WAGE DATA NOT ACCESSED 5
1. Medicaid	14	4	5	2	15
2. AFDC	28	3	8	1	7
3. Food Stamps	26	8	5	3	7

32. Currently, how compatible, if at all, is your state's automated wage reporting system with the systems of each of the programs listed below? (CHECK ONE BOX FOR EACH PROGRAM.)

	COMPATIBLE 1	SOMEWHAT COMPATIBLE 2	INCOMPATIBLE 3
1. Medicaid	26	12	6
2. AFDC	27	11	5
3. Food stamps	27	12	5

33. We would like to know how your state's privacy/confidentiality laws affect data exchanges, in general, in your state. Do your state's privacy/confidentiality laws facilitate, neither facilitate nor hinder, or hinder these exchanges, in general? (CHECK ONE.)

1. [1]greatly facilitate

2. [4]somewhat facilitate

3. [31]neither facilitate nor hinder

4. [7]somewhat hinder

5. [7]greatly hinder

34. Consider the Medicaid, AFDC, and Food Stamps programs in your state. Which of the statements below best describes how these programs are administered in your state? (CHECK ONE.)

1. [41]All three programs are administered by the same department --►(SKIP TO QUESTION 36.)

2. [9]Two out of the three programs are administered by the same department

3. [0]Each of the three programs is administered by a different department

35. Consider the fact that not all of these needs-based programs are administered by the same department in your state. Does this facilitate, neither facilitate nor hinder, or hinder data exchanges, in general, between these programs? (CHECK ONE.)

1. [0]greatly facilitates

2. [0]somewhat facilitates

3. [7]neither facilitates nor hinders

4. [1]somewhat hinders

5. [1]greatly hinders

VI. DEFRA 10 DAY ACTION DEADLINE

16. Listed below are four procedures associated with handling the tax data provided to the states by IRS and SSA. We would like to know how, and at what level, each will be performed under the system your state will implement by 10/1/86.

In SECTION A indicate whether each procedure will be done manually or automatically. (CHECK ONE BOX FOR EACH PROCEDURE.)

In SECTION B indicate at what level each procedure will be performed in your state. (CHECK ONE BOX FOR EACH PROCEDURE.)

	SECTION A HOW PROCEDURE WILL BE PERFORMED			SECTION B LEVEL AT WHICH PROCEDURE WILL BE PERFORMED		
	MOST OFTEN MANUALLY 1	AS OFTEN MANUALLY AS AUTOMATICALLY 2	MOST OFTEN AUTOMATICALLY 3	MOST OFTEN AT THE ELIGIBILITY WORKER LEVEL 4	AS OFTEN AT THE ELIGIBILITY WORKER LEVEL AS ABOVE 5	MOST OFTEN ABOVE TH ELIGIBILITY WORKER LEVEL 6
1. Screening to eliminate cases where client-provided and IRS data agree	33	7	10	33	2	15
2. Screening to eliminate cases where client-provided and SSA data agree	27	12	11	31	4	13
3. Third party validation of cases where client-provided and IRS data are discrepant	46	4	0	42	3	5
4. Third party validation of cases where client-provided and SSA data are discrepant	45	5	0	43	4	3

37. Do you anticipate, initially, greater numbers of cases that require followup than you expect as the program progresses? (CHECK ONE.)

1. [23]Definitely yes

2. [2[illegible]]Probably yes

3. [4]Probably no-►(SKIP TO QUESTION 43.)

4. [0]Definitely no-►(SKIP TO QUESTION 43.)

38. In approximately what proportion of the initial cases identified with federal data will your state realistically be able to take action within 30 days after receipt of this data? (CHECK ONE.)

1. [1]80-100%--all or almost all cases

2. [9]60-79%--most cases

3. [18]40-59%--about half the cases

4. [11]20-39%--some cases

5. [4]0-19%--few, if any, cases

39. Will your state have enough staff on hand to follow up on and complete most of these initial cases within the 30 day timeframe? (CHECK ONE.)

1. [0]Definitely yes-►(SKIP TO QUESTION 43.)

2. [7]Probably yes-►(SKIP TO QUESTION 43.)

3. [20]Probably no

4. [19]Definitely no

40. Indicate whether or not your state is planning to deal with this staff shortage in each of the following ways. (CHECK ONE BOX IN EACH ROW.)

	YES	NO
	1	2
1. Seek funding for additional staff	15	23
2. Divert staff from other functions	14	24
3. Make your best effort to meet 30 day deadline with staff on hand	34	4
4. Prioritize cases	32	6
5. Contract for services	0	38
6. Other (SPECIFY.) ________ ________	1	37

41. According to your state's due process laws, how many days is each type of program recipient listed below given to respond to an adverse action notice? (ENTER NUMBER FOR EACH TYPE OF RECIPIENT.)

	NUMBER OF DAYS TO RESPOND
1. Medicaid	10 days - 30 11-20 days - 6 Over 20 days - 2
2. AFDC	10 days - 30 11-20 days - 6 Over 20 days - 5
3. Food stamps	10 days - 11-20 days - Over 20 days -

42. Indicate whether or not your state plans to take each of the actions listed below, once your state IEVS is fully implemented, to attempt to reconcile the DEFRA 30 day action deadline with your state's right to due process laws. (CHECK ONE BOX FOR EACH ACTION.

	DEFINITLY YES 1	PROBABLY YES 2	UNCERTAIN 3	PROBABLY NO 4	DEFINITLY NO 5
1. Streamline the case follow-up process to shorten case processing time	12	18	10	9	2
2. Increase the number of eligibility workers	1	1	14	17	17
3. Make the best effort to comply with DEFRA as well as state laws given available resources	33	14	3	0	1
4. Other (SPECIFY.) 4 states responded					

VII. EXCHANGING NEEDS-BASED PROGRAM DATA WITH OTHER STATES

43. With how many states does your state currently have an ongoing agreement for the exchange of needs-based program data? (ENTER NUMBER. IF NONE, ENTER "0".)

0 states - 34
1 " - 4
2 " - 8
4 " - 1
5 " - 1
6 " - 2
15 " - 1

44. In how many of these agreements are there specific provisions safeguarding the confidentiality of the data exchanged? (ENTER NUMBER. IF NONE, ENTER "0".)

0 agreements - 37
1 " - 4
2 " - 6
5 " - 1
6 " - 2
15 " - 1

45. Listed below are factors that might affect two states' ability to reach an IEVS data exchange agreement. Indicate what effect, if any, each has on your state's ability to reach such agreements. (CHECK ONE BOX FOR EACH FACTOR.)

	GREATLY IMPEDES 1	SOMEWHAT IMPEDES 2	NEITHER IMPEDES NOR PROMOTES 3	SOMEWHAT PROMOTES 4	GREATLY PROMOTES 5
1. States' privacy/confidentiality laws	5	16	25	2	0
2. Compatibility of states' computer systems	9	20	17	2	1
3. One of the two states may discourage interstate exchanges	16	18	14	1	0
4. Compatibility of states' record file layouts	11	21	14	2	1
5. Other (SPECIFY.) 1 state responded					

46. In your opinion, which of these factors is the greatest impediment to your state's ability to reach IEVS data exchange agreements with other states? (CHECK ONE.)

1. [3] States' privacy/confidentiality laws
2. [15] Compatibility of states' computer systems
3. [12] One of the two states might discourage interstate exchanges
4. [8] Compatibility of states' record file formats
5. [11] Other (SPECIFY.)

____

____

47. Please describe any other reasons why your state has difficulty reaching data exchange agreements with other states.

18 states commented

VIII. CASE VOLUME & DISPOSITION TRACKING SYSTEM

48. DEFRA regulations require states to establish a system to annually account for the volume and disposition of cases identified through an IEVS. Which of the statements listed below best describes how your state plans to account for record volume and case action to comply with this DEFRA requirement by 10/1/86? (CHECK ONE.)

1. [8] Both record volume accounting and case action tracking will be done manually
2. [1] Record volume accounting will be done manually; case action tracking will be automated
3. [22] Record volume accounting will be automated; case action tracking will be done manually
4. [19] Both record volume accounting and case action tracking will be automated

IX. STATE'S USE OF IRS AND SSA TAX DATA

49. Has your state signed final tax data exchange agreements with the IRS and/or SSA? (CHECK ONE.)

1. [18]Signed agreement with IRS but not SSA
2. [20]Signed agreements with both IRS and SSA
3. [13]Signed agreement with SSA but not IRS
4. [10] Did not sign agreement with IRS or SSA.

50. Indicate the statement that best describes what your state will have to do to meet the safeguarding agreements for each of the four types of tax data listed below. (CHECK ONE BOX FOR EACH TYPE OF DATA.)

	ADOPT/ CREATE NEW SYSTEM	EXTENSIVELY CHANGE EXISTING SYSTEM	MODERATELY CHANGE EXISTING SYSTEM	MINIMALLY CHANGE EXISTING SYSTEM	USE EXISTING SYSTEM AS IT STANDS
	1	2	3	4	5
1. IRS unearned income data	17	7	15	5	5
2. SSA wage data	7	6	15	9	13
3. SSA private pension data	7	6	14	9	14
4. SSA self-employment income data	9	7	13	8	13

51. In SECTION A indicate how often, if ever, case files from each of the programs listed below contain historical income data that can be compared with older IRS and SSA tax data? (CHECK ONE BOX FOR EACH PROGRAM.)

In SECTION B indicate whether or not this historical case income data is automated when it is available. (CHECK ONE BOX FOR EACH PROGRAM.)

	SECTION A CASEFILES CONTAIN HISTORICAL CASE INCOME DATA... (CHECK ONE.)			SECTION B HISTORICAL CASE INCOME DATA AUTOMATED? (CHECK ONE.)		
	ALWAYS OR ALMOST ALWAYS	SOMETIMES	RARELY, IF EVER	YES	NO	NOT APPLICABLE CASE DATA RARELY, IF EVER, EXISTS
	1	2	3	4	5	6
1. Medicaid	28	15	7	9	36	5
2. AFDC	28	15	8	11	34	6
3. Food stamps	28	15	7	12	33	5

X. ADDITIONAL INFORMATION

52. Beyond its base requirements, DEFRA also encourages states to access and use other sources of information to verify the eligibility of program applicants/recipients.

In SECTION A indicate whether or not your state currently uses, or is planning to use each of the information sources listed below for eligibility verification. (CHECK ONE BOX FOR EACH SOURCE.)

For each source your state is currently using, indicate in SECTION B whether the eligibility verification process is most often automated or manual. (CHECK ONE BOX FOR EACH SOURCE YOUR STATE CURRENTLY USES.)

	SECTION A STATE CURRENTLY USES?			SECTION B VERIFICATION PROCESS...		
	YES, STATE CURRENTLY USES	NO, BUT STATE PLANS TO USE	STATE NEITHER USES NOR PLANS TO USE	AUTOMATED ON-LINE	AUTOMATED OFF-LINE	MANUAL
	1	2	3	4	5	6
1. Birth records	33	3	14	5	0	30
2. Death records	30	3	17	3	5	25
3. Marriage records	27	2	21	1	0	27
4. Divorce records	26	2	22	1	0	26
5. Drivers' license records	25	4	20	8	6	12
6. Auto registration records	33	9	8	16	10	13
7. Selective service records	5	0	44	0	0	5
8. Police records	11	1	37	1	2	9
9. Tax records (other than fed.)	14	8	26	1	3	12
10. Housing records	18	4	28	1	0	18
11. Bank records	32	6	12	1	4	29
12. Insurance records	21	1	25	0	2	22
13. Credit records	13	0	36	1	3	9
14. Other (SPECIFY.) 10 states responded						

53. In responding to the cost vs. benefit questions earlier in this questionnaire, were any of your responses based on actual studies or analyses your state has done?

1.[13]Yes

2.[38]No--(SKIP TO QUESTION 55.)

54. We are interested in obtaining the results of any cost/benefit studies or analyses your state has done, related to the DEFRA, IEVS provisions. However, we would like you to give priority to the completion and return of this questionnaire. Under separate cover and at your convenience, please send a copy of such reports to us at the address shown on the front of this form.

1 study received

55. Please write comments you might have about the DEFRA regulations, in general, or its provisions or impact, in particular, in the space below.

19 states commented

GAO

United States General Accounting Office

Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations
House of Representatives

August 1986

PRIVACY ACT

Federal Agencies' Implementation Can Be Improved

GAO/GGD-86-107

Executive Summary

Purpose

Federal agencies collect and use virtually billions of records containing personal information on individuals. The possession of such vast quantities of personal information has raised public and congressional concerns over the ability to protect and balance the privacy of individuals in relation to the information needs of government. This concern has grown as expanding information technologies are providing for faster, broader, and less expensive access to these sensitive records.

GAO was requested by the Chairman, Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, to examine agencies' implementation of the Privacy Act of 1974, the principal law aimed at protecting personal privacy. This report provides an analysis of how agencies have (1) organized their Privacy Act activities and (2) followed selected provisions of the act and Office of Management and Budget (OMB) implementing guidelines.

Background

The Privacy Act of 1974 provides certain safeguards to individuals against invasion of privacy by requiring federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems.

A basic premise of the law is that information about individuals should not be maintained in secret files. With some exceptions, individuals have the right to (1) know what records pertaining to them are collected, maintained, used, and disseminated by the agencies; (2) have access to agencies' information pertaining to them and to amend or correct the information; and (3) prevent information obtained by agencies for a specific purpose from being disclosed for another purpose without their consent.

The act also requires agencies to insure that any records of identifiable personal information they maintain are for necessary and relevant purposes, that they are current and accurate for their intended uses, and that adequate safeguards are provided to prevent misuse of such information. Each agency is responsible for implementing the act with guidance and oversight from OMB. (See pp. 8 to 10.)

GAO examined organizational issues at 13 Cabinet-level departments and the Veterans Administration and reviewed Privacy Act operations in detail at six of these agencies and 37 of their components.

Results in Brief

Agencies have taken highly decentralized approaches to implementing the law and often have not established clear lines of responsibility and accountability for Privacy Act functions. All of the 14 agencies had Privacy Act officers or their equivalent; however, the officers' limited responsibilities and resources indicated that they did not exercise the oversight originally envisioned by OMB. At the six agencies GAO reviewed in detail, improvements were needed in adhering to OMB guidance relating to such activities as computer matching programs, risk assessments, evaluations, and training.

Clearer Responsibility and Accountability Needed

The degree to which Privacy Act responsibilities were clearly delineated and accountability established varied widely among the agencies. Three of the 14 agencies did not have agencywide directives specifying responsibilities. The other 11 agencies had published directives, but they generally lacked detail and specificity. For example, Privacy Act functions such as computer matching, compliance evaluations, and training were frequently not addressed in the directives. (See pp. 15 to 17.)

Privacy Act Officers Have Limited Roles

The position of Privacy Act officer was established to provide coordination and oversight of Privacy Act implementation. GAO's analysis of agency directives and position descriptions, however, showed that significant functions such as ensuring compliance and providing Privacy Act training were not always assigned. Even if these and other responsibilities were assigned, it is doubtful that the Privacy Act officers could carry them out given the resources made available to them. These individuals generally held mid-level management positions and conducted Privacy Act activities on a part-time basis, in 10 agencies less than half-time. Five officers had no staff resources. Of the nine who had assistants, seven had fewer than the full-time equivalent of 1 staff. (See pp. 18 to 22.)

Many Improvements Needed at the Six Agencies Reviewed in Detail

While OMB asks agencies to conduct detailed risk assessments for newly created or modified record systems to assure security and confidentiality, the six agencies in GAO's detailed review could provide evidence of an assessment for only 1 of 27 record systems. Five of the six agencies did not report accurate data to OMB on the extent of their computer matching activities. In addition, of 26 computer matching programs, 6 did not follow OMB guidance. The training needs of the hundreds of individuals responsible for Privacy Act compliance had not been assessed or provided in a systematic manner. The agencies did not routinely conduct internal evaluations of Privacy Act operations. Where matching and other activities related to the Privacy Act were conducted, Privacy Act officers at both agency and component levels were frequently unaware of and uninvolved in them. (See ch. 3.)

Recommendations

Because of OMB's key role in managing executive branch operations and in light of the responsibilities assigned to it by the Privacy Act, GAO makes a number of recommendations to OMB for improvement in oversight, agency evaluation, and OMB guidelines pertaining to such activities as computer matching programs. (See pp. 48 to 49.)

Agency Comments

OMB said it believes GAO's recommendations are reasonable and has been working to implement some of them. OMB's other comments concerned such areas as the Paperwork Reduction Act, the role of Privacy Act officers in relation to senior officials, and the impact of concurrent responsibilities on Privacy Act officers' duties. (See pp. 49 to 50.)

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON OFFICE

ACLU PRIVACY AND TECHNOLOGY PROJECT
SEPTEMBER 1985

MEMORANDUM

TO: Conferees and Interested Persons

FROM: Jerry J. Berman and Lauren Dame

RE: Computer Matching--FOCUS PAPER
For September 1985 Consultation

I. Introduction

Computer matching is a process whereby separate files are run through a computer with a program set to detect predetermined "matches"--i.e., the same information present in both files. Since the 1970's, the government has been using computer matching as a technique to compare unrelated government files in order to detect fraud and abuse in government programs. For example, state unemployment compensation records have been compared with employers' quarterly wage reports to detect people receiving unemployment compensation and also earning a salary.

Ever since the government began using computer matching, there has been a debate between those who view it as an efficient auditing tool, and those who view it as a serious threat to privacy and civil liberties. In the initial debates concerning computer matching, the two sides found it useful to argue the case in stark terms. But today, the debate needs to be reformulated in order to consolidate the gains made by early opponents, and to move towards an understanding of the nature of the problem today. In much of the debate so far, the two sides have not always clearly separated different issues about computer matching such as the type of computer matching they are talking about, and the specific concern raised by each type. The term "computer matching" has been applied to a wide range of data processing techniques involving computers, but each technique raises distinct problems. Failure to distinguish among different types of computer matches has caused some confusion.

The other source of confusion in the computer matching debates has been a failure on the part of some opponents of computer matching to distinguish between two distinct categories of concerns about computer matching. The first category has to do with the fairness of a particular match: how it is organized and carried out; what sort of notice people are given; what types of hearings one gets before benefits are cut off; etc. People may be strongly in favor of increasing the use of computers by the government, yet think that matches must be performed "fairly."

The second category of concern is about the longterm effects of massive computerization and computer linkages, and involves fundamental civil liberties issues as well as philosophical concerns about the type of society we may be creating. It is here that the conflict between the fundamental values of the proponents and opponents of computer matching is most starkly presented. Computer matching proponents consider efficiency to be a fundamental value, while those opposed to computer matching value qualities of individuality and privacy.

II. Purpose of this Paper

The purpose of this paper is to break apart the different issues and concerns raised by computer matching, and to work towards developing a coherent policy. Only by understanding the variety of problems posed by computer matching can we intelligently chose among the options facing us. This paper is designed to raise issues, options, and make suggestions, but is not intended to present any final conclusions. We are still in the process ourselves of analyzing the complex problems posed by computer matching, and would appreciate comments about whether our analysis so far is coherent and useful.

III. Computer Matching

1. Defining computer matching

"Computer matching" is a term that has been applied to a variety of computerized data processing activities where separate files are run through a computer with a program set to detect certain "matches." When a piece of information is found to be in both databases, (for example, the same name or social security number) it is called a "raw hit", and provides the starting point for further action on the part of the agency doing the computer match. This process of computer matching is being used by government agencies to detect fraud and abuse in government programs by linking together formerly independent databases. The nature of a computer match can range in complexity from a simple match of social security numbers, to a selection of all people in a file who have a certain combination of characteristics.

Some computer matches are merely more efficient ways of comparing two lists--an activity that could have been done even before the days of computer matching. Other matches involve searches through such a complex number of variables that they would not be possible without a computer. In either case, however, it is only with the spread of computer technology that it has become worthwhile for the government to conduct these searches. In the first type of match, the physical difficulty of manually going through millions of names in separate files served as a threshold barrier to excessive government policing. Now, however, because of computer technology, this important limitation no longer exists.

To fight against all "computer matching" is to fight a losing battle--computers have entered the workplace, and it is unrealistic to expect the government not to use them.*

Therefore, we must focus on the type of computer matching that seems to raise the most serious concerns. The matching of personally identifiable information from two or more files raises both privacy issues and, because of linkage among disparate databases, the spectre of a de facto national database. This is the type of computer matching that we are most concerned about and that we will use as our definition of computer matching.

A well-known example of this type of computer matching occurred in Massachusetts in 1982, when the state department of public welfare gave its computer lists bearing the social security numbers ["SSNs"] of all welfare recipients in the state to the major Massachusetts banks. The banks were asked to match the welfare tapes with their records to identify any welfare recipient who had cash assets beyond the allowable limit for people on welfare. A list of "raw hits" was generated, and Massachusetts terminated the benefits of those welfare recipients who appeared on it. It was later discovered that there were many legitimate reasons why welfare recipients showed up on the list. Some appeared because inaccurate social security numbers on the bank records falsely indicated that the welfare recipients had accounts when in fact they did not; other welfare recipients appeared because they had assets over the limit, but the assets turned out to be for things specifically exempted by law, such as burial expenses held in trust. (It was later determined that 24% of the SSNs used in the match were incorrect. US Senate 1982, p. 224.)

---

*The ACLU even uses computer matching techniques. To counter Administration claims that no deportees have been retaliated against back in El Salvador, the ACLU Political Asylum Project used computer matching to match lists from INS of Salvadoran deportees with lists of victims of human rights abuses.

In addition to the process of "comparing" two or more databases, there are two other techniques often lumped under the rubric of "computer matching": "front-end verification" and "profiling." Because these techniques are often used in conjunction with computer matching, and are sometimes suggested as alternatives to computer matching, they are also discussed in this paper. Both techniques, however, raise some distinct problems of their own.

Front-End Verification

Front-end verification is a procedure for checking the accuracy and truthfulness of an application when a person first applies for a government program. The application is matched against other records maintained by the government to determine if other information about the applicant is available. Thus, an application for welfare might be matched with files of bank accounts to check for assets beyond the amount permitted, or with employer wage reports to check that the income reported on the application is correct.

Front-end verification has been called less intrusive than computer matching because only the applicant's file is checked, rather than all the files in a particular database. In addition, it catches errors before benefits are paid, and perhaps before any fraud is committed. Government agencies currently using computer matching programs hope to replace these programs with front-end verification once ineligible recipients have been "weeded out" by computer matching. However, they admit that front-end verification will not completely replace computer matching because error or fraud can occur after an applicant is initially certified eligible for assistance.

The INS and a few state welfare departments are currently conducting a pilot front-end verification program called "SAVE". (Systematic Alien Verification for Entitlements.) In this program, welfare applications from aliens are compared with computerized INS listings to check whether the applicant is listed in INS databases as a legal alien. Illegal aliens are thus detected and kept off the welfare rolls.

Without SAVE, state welfare departments check the status of aliens through a time-consuming process of sending forms to INS. Since state welfare laws often require a state to accept or reject an applicant within 10 days, a state may have to pay benefits until it receives an answer from INS that the alien is ineligible. It then has to initiate formal proceedings to revoke the benefits. With SAVE and computerization, verification could occur within ten days, so the illegal alien would not get on the rolls in the first place.

This project points out some of the problems with computer matching and front-end verification in general. Although it could be used to speed up processing of welfare applications, and as such, be a benefit to eligible applicants, the program has been designed foremost as a "policing" tool. As the INS said in a memorandum about SAVE, "success will be measured by the number of criminal prosecutions resulting from these efforts; the dollars of cost avoidance; and the number of unentitled aliens identified and removed or barred from benefit rolls." The built-in "policing bias" seems to ensure that mistakes that occur in the system will be tilted towards keeping eligible people out of the program incorrectly, rather than accepting ineligible people incorrectly. Thus, while illegal aliens may well be successfully prevented from getting on the welfare rolls, other aliens who are eligible may be falsely denied benefits because of errors in INS records. These false denials can be serious when the applicant seeks benefits necessary for the most basic subsistence. In addition, eligible aliens may be scared away from applying for benefits in the first place because of misinformation about their eligibility or fear of the INS.

Because an important goal of front-end verification is to increase the speed and exchange of information among government agencies, there is pressure in these programs to increase computer-to-computer connections and on-line processing. HHS describes a front-end system planned by the Michigan Department of Social Services:

"Within two years, it intends to have in place an integrated front-end system which incorporates four major data sources and is accessible on-line in all field offices. The data sources that could be tapped for any applicant would be from the State Department of Treasury, the Secretary of State's office, the State Department of Employment Security, and the State Department of Management and Budget. They would provide eligibility assistance workers with information on state income tax returns, registered motor vehicles, unemployment compensation benefits, and state government employees."

While front-end verification solves some of the problems of computer matching by making the search individualized, it also pushes towards a centralized data bank, as the passage above indicates. By connecting these disparate records together, the government creates the illusion of an all-knowing "Big Brother." The fear this induces in people may have negative consequences for the government when it suddenly needs people to trust it. (There may be times when it is important for citizens and aliens to participate in government activities, such as census taking or programs to eradicate health hazards. By instilling a fear that all information collected by one government agency is going to find its way into other agencies, we may be creating an atmosphere of distrust that will hurt our nation deeply.)

Profiling

Profiling is a technique in which the computer looks for a certain combination of data items. Although no single item alone indicates anything wrong, a pattern of all the items may indicate fraud or abuse. The most simple form of profiling is a "laundry list" of items and when a certain number of them occur in one person's file, that file would be pulled for further examination. For example, HHS developed a profile to detect "welfare queens" -- women who receive AFDC payments for non-existent children. The computer looks for people who match the profile, which includes such items as a large number of children, no record of medicaid payments for children's medical expenses, and no listing of the children in a school.

Although profiling can be useful to narrow the number of "hits" that a computer match will produce, the use of such profiles raises questions about whether we want to use certain items in our profiles (such as race, or religion), and whether we want to promote the use of stereotypes.

2. Brief History and Current Status

Computer matching by government agencies gained popularity in the late 70's. Before 1976, there were few computer matching programs by government agencies. In 1977, the Carter administration initiated "Project Match", a computer matching scheme which involved comparing HEW's computer tapes of welfare recipients with federal payroll files in a number of states. The goal was to detect government employees who were fraudulently receiving welfare benefits. The program required the use of computer files from HEW, the US Civil Service Commission, and DOD.

It is unclear exactly how much computer matching is going on today, for the recordkeeping is scattered and incomplete. The GAO estimates that, since 1976, federal agencies have initiated over 125 matches (some recurring) and state agencies have initiated over 1,200. (Other estimates are much greater, due in part to differences in how recurring matches are counted, and due in part to the difficulty of getting accurate information.) In any case, it is clear that the use of computer matching is growing. In 1982, President Reagan established the President's Council on Integrity & Efficiency (PCIE) to combat fraud and waste in government programs. The Council seems quite enamored with computer matching, and one of its major activities is the Long Term Computer Matching Project, aimed at improving the use of computer matching in government. The Council is also involved in efforts to standardize data formats among government agencies -- a step which will facilitate computer matching of files. These factors all indicate that computer matching will become even more common in the future, and that more databases will be linked because of common formats.[*]

---

[*] In addition, since common formats rely on some sort of universal identifiers, this will push the drive for identifiers such as the fraud-proof identifiers proposed in different immigration reform legislation.

In addition, federal laws have been passed which require states to do computer matching as a condition of receiving certain federal funds. For example, the Deficit Reduction Act of 1984 requires state agencies that administer the Food Stamp, AFDC, SSI, and medicaid programs to check the eligibility of recipients and applicants by running computer matches of state welfare records with wage reports from private employers and unearned income reports from the IRS.

3. The Current Law: Are There Any Limits on Computer Matching?

The Privacy Act of 1974, 5 U.S.C. §552a, was passed as a result of concern over the growing amount of data about individuals being collected and maintained by the government. In fact, one of the purposes of the Act was to deal with the privacy problems raised by computers:

> The Congress finds that. . .the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information. [Privacy Act, Section 2(a)(2)]

The Act regulates the collection, maintenance and dissemination of government records containing information about an individual, and, amohg other things, prohibits the disclosure of these records without the permission of the person concerned. The Act contains 11 exception to this disclosure prohibition, however, and these exceptions have proven to be so broad as to vitiate much of the protection initially promised by the Act.

In the area of computer matching, the most important exception is the "routine use" exception. [5 U.S.C. §552a(b)(3)] This exception provides that a record covered by the Act may be disclosed if disclosure would be for a "routine use," defined as the use of a record for a purpose which is compatible with the purpose for which the record was originally collected. The language of the "routine use" exception does not seem to permit an agency to release information in payroll records, collected for employment purposes, to another agency to be used in detecting welfare fraud. In fact, this point was raised by Carl Goodman, General Counsel of the U.S. Civil Service Commission, in response to HEW's request for his agency's files in order to perform "Operation Match". In his June 1977 letter to HEW, he stated:

> At subsection (a)(7) of the Act, "routine use" is defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected." Although the literal terms of this provision obviously cannot be

> followed with precision in practical application of agency operations, it is evident that this information on employees was not collected with a view toward detecting welfare abuses.

However, government agencies have argued that detecting fraud and abuse in government programs is a "legitimate government purpose", and thus is compatible with any original "legitimate government purpose" for which the records were collected in the first place. Thus, the routine use exception has made the Privacy Act fairly meaningless in terms of protecting records from computer matching programs.

The OMB has prepared guidelines for agencies to follow in conducting computer matching projects. Although the guidelines are supposed to help protect individuals' privacy, there is only minimal oversight of computer matching projects by OMB, and with no enforcement mechanisms provided, the agencies have not been greatly restrained by these guidelines. In addition, government agencies have gotten around the Privacy Act's requirement of "notice" by declaring that sufficient notice is given when the agency publishes an announcement of the match in the Federal Register.

As to the current state of the law, this is an area where technology has outpaced legal developments, and the spread of wide-ranging computer matching has gone on relatively unchecked. There are privacy provisions in a number of different laws, which provide limited protection for specific records, (for example, the Tax Reform Act of 1976 restricts the disclosure of tax return information), and some due process provisions were included in the Deficit Reduction Act of 1984, requiring "human" verification of "hits" generated by a match before terminating benefits. (These provisions are to take care of the types of problems that occurred in the Massachusetts program, described earlier.) Besides the due process provisions, a positive aspect of the Deficit Reduction Act is the fact that by specifically mandating certain matches, it provides some statutory authority for the argument that the "routine use" exception to the Privacy Act does not justify all matches.

IV. Concerns Raised by Computer Matching & Policy Options

The goal of many computer matching projects is a legitimate effort to track down and reduce waste and fraud in government programs, but the government's position seems to be that privacy concerns should be secondary to efficiency concerns. Many civil libertarians disagree, and think that computer matching raises a number of serious issues. One of the best examples of how the present debate over computer matching is argued on both sides is the Shattuck-Kusserow exchange in "Computer Matching: Should It Be Banned?", Communications of the ACM, June 1984. While we still agree with the concerns expressed by John Shattuck, we think that the arguments by opponents to computer matching have to be reconceptualized and broken apart in order to draw out more fully the implications of the arguments made and solutions proposed. The broadside attack on computer matching has caused proponents of computer matching to make a number of concessions, and to include some due process protections in matches. For example, as Richard Kussrow explains in this article, no longer are benefits terminated solely on the basis of a "match" without some sort of further verification. Based on numerous articles about computer matching, we have summarized below some of the key arguments made against computer matching, and some questions about the way the problems have been conceptualized.

1. UNREASONABLE SEARCH & SEIZURE

The Fourth Amendment protects against unreasonable searches and seizures, and embodies a principle against government "fishing expeditions" in which large numbers of people are investigated without any specific evidence that any particular individual has committed a crime. Computer matching, however, is often just such a fishing expedition. The records of hundreds or even thousands of people are searched with the hope that some evidence of wrongdoing might show up.

Is a fourth amendment "unreasonable search and seizure" analysis still useful in this area given, current fourth amendment doctrine? Is it realistic to compare a computer's scan of a computer tape with a general search? Some argue that computer matching is not an unreasonable search and seizure--there are many examples where law enforcement activity legitimately involves a general scan of information relating to individuals without prior evidence of wrongdoing. For example, many states require all automobiles to display current vehicle inspection stickers and the police routinely visually scan vehicles without any reason to suspect that any particular vehicle is in violation. Also, the IRS routinely reviews income tax returns from individuals without any evidence of wrongdoing by the individual.

Although one can make an interesting fourth amendment argument against computer matching, current fourth amendment doctrine goes in the opposite direction. The courts have held constitutional a wide range of categorical searches, such as the use of an "area" warrant to support the reasonableness of routine inspections of private residences for building code violations, and searches of automobiles by INS at fixed checkpoints inside the US border to check for illegal aliens. [*Camara v. Municipal Court*, 387 US 523 (1967); *US v. Martinez-Fuerte*, 328 US 543 (1976)] Summarizing the fourth amendment's individualized suspicion requirement, the Supreme Court stated that although some quantity of individualized suspicion is usually a prerequisite to a constitutional search, "the Fourth Amendment imposes no irreducible requirement of such suspicion. [Citations omitted.] Exceptions to the requirement of individualized suspicion are generally appropriate only where the privacy interests implicated by a search are minimal and where 'other safeguards' are available 'to assure that the individual's reasonable expectation of privacy is not subject to the discretion of the official in the field.'" [New Jersey v. T.L.O., 105 S. Ct. 733, 744 note 8 (1985).]

Making the argument that a fourth amendment right is being violated by the process of computer matching is especially difficult in light of the Supreme Court's holding in United States v. Miller, 425 US 435 (1976), that an individual has no privacy interest in records held by third parties.

The National Security Agency (NSA) currently collects all international microwave and radio communications, and it could be argued that this is a "general search." However, in Jabara v. Webster, (S. Ct. No. 82-1682, 1983), the ACLU felt that it had to argue that a fourth amendment search occurred only when a specific person was targeted, and his or her private communications were then translated from machine storage into readable form and read by NSA; that the mere monitoring and collection of communications did not violate his or her privacy as long as the contents of private communications were not read. Analogizing this to computer matching would suggest that a person's record is not "searched" until after a hit, and his or her record is specifically examined.

Policy Options

One policy option is to completely ban computer matching by the government, but there are several problems with this as a solution. First, one would still need to distinguish between the kinds of computer matching that pose privacy problems and the kinds of computer matching that are mere technologically advanced ways of doing things the government is already doing. Otherwise the objections do not seem to be against computer matching, but rather against technology altogether. In addition, given how widespread computer matching already is, banning it all together does not seem realistic. (Especially in a political climate that is more interested in cutting back expenditures than in protecting civil liberties.) Another point we must seriously consider is the claim that, if you are going to permit the government to perform audits, then automated audits using computer matching are LESS intrusive, and more efficient than manual ones.

2. INNOCENT UNTIL PROVEN GUILTY

A basic tenet of our legal system holds that people are presumed innocent until proven guilty. When a person is denied a benefit because his or her name appears on a "hit" list generated by a computer match, this presumption of innocence is turned on its head. The person is presumed guilty of fraud and must prove his innocence, sometimes fighting through an elaborate appeals process.

Is this a problem with computer matching itself, or merely with the action taken as a result of the match? Is a "raw hit" in a computer match merely one piece of evidence, the same as an anonymous tip, a fingerprint, or any other single indicator of guilt? Or is the "scientific veneer" attached to computers so compelling that the tendency in computer matches will be to consider the computer "correct" and force the hapless victims to prove their innocence. We have all experienced the frustrations of trying to convince a bureaucrat that his or her machine has made a mistake -- will computer matching, by its very nature, increase this type of problem?

It seems that the argument that computer matching turns the presumption of innocence into a presumption of guilt holds up only if a person is denied a benefit solely on the basis of a "hit", something which did occur in the Massachusetts match. However, that match occurred in 1982, and although it is the favorite "horror story" of computer matching opponents, reports today suggest that government agencies conducting computer matches have become more sophisticated and no longer deny benefits or take final actions solely on the basis of a "hit." Is there still anything left to this presumption of innocence argument if that is true? (Does anyone know of other, current matches in which actions were taken solely on the basis of the computer's results?)

Policy Options

One option to take care of these concerns about the presumption of innocence would be to require human verification in all matching programs before any benefits can be terminated or denied. This would take care of the "presumption of innocence" problem, but would push the drive towards front-end verification, which in turn produces other problems. In addition, a way to avoid numerous "hits", all of which require verification, would be to increase the amount and accuracy of information that the computer contains in the first place, and thus avoid a portion of hits caused by inadequate information. But this kind of action obviously contains a cost, for it takes us further down the road towards more and more personal and accurate information being kept in computerized records.

3. DUE PROCESS

Due process of law has to do with treating fairly those individuals faced with the power of the government and its legal system. It includes the right to confront one's accusers, and to introduce evidence on one's behalf. In a computer matching program, these basic elements of due process are often not available until well after the government has moved against the individual. Rarely do recipients of government benefits have an opportunity to examine their records to make sure that the information contained is accurate, and often they do not learn of a computer matching program until they are investigated by the government because their names appear on a "hit" list. In some cases, such as the Massachusetts case described earlier, the individuals are given no notice of the match until their benefits are terminated.

Policy Option

Several things could be done to reduce these due process problems:

1. Require *explicit* notice on application forms and other government forms that the file is subject to verification and to matching with files held by other government agencies. The Code of Fair Information Practices, a set of principles proposed by HEW in 1973, includes the principles that an individual should be able to find out what personal information is collected, how it is used, and that it should not be used for a new purpose without his or her consent. Some government officials argue that applicants are already given "notice", but this is debatable. For example, the following appeared on a veterans' benefits application form:

"The information submitted may be disclosed outside the Veterans Administration [VA] only as permitted by law, including the routine uses identified in VA system of records 58VA 21/22/28, Compensation, Pension, Education and Rehabilitation Records--VA published in the *Federal Register*."

Requiring better notice of verification and giving notice to applicants that they have the right to see and correct their files would help improve due process problems.

2. Require independent verification of all "hits" before further action is taken.

3. Require a hearing before any benefits are denied or terminated.

4. PRIVACY ACT

The most important principle governing collection and use of personal information by the government is that the individual has a right to control information about his or herself and to prevent its use without his or her consent for purposes wholly unrelated to those for which it was collected. This bedrock principle of individual privacy is imperfectly embodied in the Privacy Act of 1974, and is violated by the practice of computer matching.

As we said earlier, the history and rhetoric of the Privacy Act suggest that Congress thought that it was prohibiting computer matching of unrelated files, (the type of matching we have defined as the most serious), when it passed the Privacy Act. Yet over the years, government agencies have interpreted the "routine use exception" of the Privacy Act to permit computer matching, and now the Privacy Act offers little protection from computer matching.

One option is to support legislation that computer matching does not fall within the routine use exception of the Privacy Act, and to strengthen the original intention of the Act. Provisions could be incorporated into the Privacy Act to prohibit *any* computer matching with certain records (such as tax records); to require Congressional authorization for matches; and to require due process provisions such as those in the Deficit Reduction Act, and the options described in the due process discussion above.

5. BIG BROTHER AND DE FACTO NATIONAL DATA CENTER

Finally, there is an overarching concern best identified as the fear of a "Big Brother" government. With computer technology, agencies are able to check through enormous numbers of files to search for any number of items, and the possibility exists of linking up previously disparate computer files to form a national database containing information on all citizens. With computer matching, the individual loses the ability to control information about him or herself, and the government is able to increase its policing of our private lives.

This concern has to do with the very nature of privacy in a society in which large amounts of information about individuals are kept in numerous government and private files. Computer matching is only a part of a movement towards a society in which information about an individual is increasingly amassed and concentrated. Our current "inefficient" system of having separate, incompatible files in many different agencies has been a form of protection up to now. The pattern of development in this country and indeed throughout the world, has been one of increasing complexity and interconnectedness. We find it useful and necessary to provide a great deal of information to a variety of institutions in order to apply for credit, jobs, benefits, etc. Individuals who wish to protect their privacy no longer have the option of keeping information to themselves unless they wish to lead strange, isolated lives.

With computer matching and what it represents, we are moving from a system relying on voluntary compliance and an assumption that citizens obey the law, to the assumption that citizens cannot be trusted. This assumption may become a self-fulfilling prophecy as people become aware of the extent to which information can be shared and they can be monitored. There will also be a drive towards conformity --both social and political-- as computers look for deviance from predetermined norms programmed into the computer.

Some argue that the concern over privacy and computers is merely a reflection of the liberal doctrine of individualism, and that the collection of data represents a return to the type of communal society of small towns where everyone knew everything about everyone else. But there is a big difference between a small town, where the citizens who know each others' faults and secrets also know each other as human beings, and have social interactions, and a central government computer used by an impersonal bureaucracy. Linking up the computers in various government agencies does not produce "community."

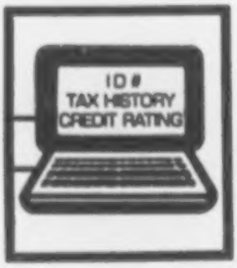
V. Analyzing the Problems and Solutions

Incremental problems with computer matching can be solved, but as we have pointed out throughout this paper, these solutions may exacerbate our larger concern about creating a Big Brother society. We can require front-end verification to avoid the "general search" aspect of computer matching, but this pushes towards centralized data bases and on-line computer connections. We can require application forms to give people notice that their file will be matched with five other databases, but this does not stop the linkage. We can demand that agencies use accurate information to reduce the number of false "hits", but this also increases the amount and accuracy of the personal information the government keeps on us.

What we need to think about are options that go to the more general concern. We must change the terms of the debate to include these larger concerns about the society we are creating. We do not have the answers, but some options to focus on include working to protect some databases from being matched at all (such as tax files, information about one's political beliefs, and other highly private information); requiring all new files created by a match to be destroyed after the match; and to prevent "matching" of files from becoming "merging" of files.

Federal Government Information Technology

Electronic Record Systems and Individual Privacy



ID #
TAX HISTORY
CREDIT RATING

CONGRESS OF THE UNITED STATES
Office of Technology Assessment
Washington, D. C. 20510

Chapter 1

Summary

INTRODUCTION

All governments collect and use personal information in order to govern. Democratic governments moderate this need with the requirements to be open to the people and accountable to the legislature, as well as to protect the privacy of individuals. Advances in information technology have greatly facilitated the collection and uses of personal information by the Federal Government, but also have made it more difficult to oversee agency practices and to protect the rights of individuals.

In 1974, Congress passed the Privacy Act to address the tension between the individual's interest in personal information and the Federal Government's collection and use of that information. The Privacy Act codified principles of fair information use that specified requirements agencies were to meet in handling personal information, as well as rights for individuals who were the subjects of that information. To ensure agency compliance with these principles, the act enabled individuals to bring civil and criminal suits if information was willfully and intentionally handled in violation of the act. In addition, the Office of Management and Budget (OMB) was assigned responsibility for overseeing agency implementation of the act.

At the time the Privacy Act was debated and enacted, there were technological limitations on the use of individual records by Federal agencies. The vast majority of record systems in Federal agencies were manual. Computers were used only to store and retrieve, not to manipulate or exchange information. It was theoretically possible to match personal information from different files, to manually verify information provided on government application forms, and to prepare a profile of a subset of individuals of interest to an agency. However, the number of records involved made such applications impractical.

In the 12 years since the Privacy Act was passed, at least two generations of information technology have become available to Federal agencies. Advances in computer and data communication technology enable agencies to collect, use, store, exchange, and manipulate individual records in electronic form. Microcomputers are now widely used in the Federal Government, vastly increasing the potential points of access to personal record systems and the creation of new systems. Computer matching and computer-assisted front-end verification are becoming routine for many Federal benefit programs, and use of computer profiling for Federal investigations is expanding. These technological advances enable agencies to manipulate and exchange entire record systems, as well as individual records, in a way not envisioned in 1974. Moreover, the widespread use of computerized databases, electronic record searches and matches, and computer networking is leading rapidly to the creation of a *de facto* national database[1] containing personal information on most Americans. And use of the social security number as a *de facto* electronic national identifier facilitates the development of this database.

These technological advances have opened up many new possibilities for improving the efficiency of government recordkeeping; the detection and prevention of fraud, waste, and abuse; and law enforcement investigations. At the same time, the opportunities for inappropriate, unauthorized, or illegal access to and use of personal information have expanded. Because of the expanded access to and use of personal information in decisions about individuals, the completeness, accuracy, and relevance of information is even more important. Additionally, the expanded access and use make it nearly impossible for individuals to learn about, let alone seek redress for, misuse of their records. Even within agencies, it is often not known what applications of personal information are being used. Nor do OMB or relevant congressional committees know whether personal information is being used in conformity with the Privacy Act.

---

[1] The term *de facto* national database is used to distinguish it from a national database that was created by law, i.e., a *de jure* national database.

Overall, OTA has concluded that Federal use of new electronic technologies in processing personal information has eroded the protections of the Privacy Act of 1974. Many of the electronic record applications being used by Federal agencies, e.g., computer profiling and front-end verification, are not explicitly covered by the act or by subsequent OMB guidelines. The rights and remedies available to the individual, as well as agency responsibilities for handling personal information, are not clear. Even where applications are covered by the Privacy Act or related OMB guidelines, there is little oversight to ensure agency compliance. More importantly, neither Congress nor the executive branch is providing a forum in which the conflicts—between privacy interests and management or law enforcement interests—generated by Federal use of new applications of information technology can be debated and resolved. Absent such a forum, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems.

POLICY PROBLEMS

OTA's analysis of Federal agency use of electronic record systems, specifically for computer matching, front-end verification, and computer profiling, revealed a number of common policy problems.

First, **new applications of personal information have undermined the goal of the Privacy Act that individuals be able to control information about themselves.** As a general principle, the Privacy Act prohibits the use of information for a purpose other than that for which it was collected without the consent of the individual. New computer and telecommunication applications for processing personal information facilitate the use of information for secondary purposes, e.g., use of Federal employee personnel information to locate student loan defaulters, or use of Federal tax information to evaluate a Medicaid claim.

The expanded use and exchange of personal information have also made it more difficult for individuals to access and amend information about themselves, as provided for in the Privacy Act. In effect, the Privacy Act gave the individual a great deal of responsibility for ensuring that personal information was not misused or incorrect. Technological advances have increased the disparity between this responsibility and the ability of the individual to monitor Federal agency practices. For example, individuals may not be aware that information about them is being used in a computer match or computer profile, unless they monitor the *Federal Register* or questions about them arise as a result of the application. In computer-assisted front-end verification, individuals may be notified on an application form that information they provide will be verified from outside sources, but are unlikely to be told which sources will be contacted.

Additionally, new computer and telecommunication capabilities enable agencies to exchange and manipulate not only discrete records, but entire record systems. At the time the Privacy Act was debated, this capability did not exist. The individual rights and remedies of the act are based on the assumption that agencies were using discrete records. Exchanges and manipulations of entire record systems make it more difficult for an individual to be aware of uses of his or her record, as those uses are generally not of immediate interest to the individual.

Second, **there is serious question as to the efficacy of the current institutional arrangements for oversight of Federal agency compliance with**

the Privacy Act and related OMB guidelines. Under the Privacy Act, Federal agencies are required to comply with certain standards and procedures in handling personal information—e.g., that the collection, maintenance, use, or dissemination of any record of identifiable personal information should be for a necessary and lawful purpose; that the information should be current, relevant, and accurate; and that adequate safeguards should be taken to prevent misuse of information.

OMB is assigned responsibility for oversight of agency implementation of the Privacy Act. Prior studies by the Privacy Protection Study Commission (1977), the U.S. General Accounting Office (1978), and the House Committee on Government Operations (1975 and 1983) have all found significant deficiencies in OMB's oversight of Privacy Act implementation. For example, under the Privacy Act, information collected for one purpose should not be used for another purpose without the permission of the individual; however, a major exemption to this requirement is if the information is for a "routine use"—one that is compatible with the purpose for which it was collected. Neither Congress nor OMB has offered guidance on what is an appropriate routine use; hence this has become a catchall exemption permitting a variety of exchanges of Federal agency information.

Looking more specifically, OTA found that OMB is not effectively monitoring such basic areas as: the quality of Privacy Act records; the protection of Privacy Act records in systems currently or potentially accessible by microcomputers; the cost-effectiveness of computer matching and other record applications; and the level of agency resources devoted to Privacy Act implementation. OTA also found that neither OMB nor any other agency or office in the Federal Government is currently collecting or maintaining this information on a regular basis. Given the almost total lack of information concerning the activities of Federal agencies with respect to personal information, OTA conducted its own one-time survey of major Federal agencies and found that:

- the quality (completeness and accuracy) of most Privacy Act record systems is unknown even to the agencies themselves; few (about 13 percent) of the record systems are audited for record quality, and the limited evidence available suggests that quality varies widely;
- even though the Federal inventory of microcomputers has increased from a few thousand in 1980 to over 100,000 in 1985, very few agencies (about 8 percent) have revised privacy guidelines with respect to microcomputers;
- few agencies reported doing cost-benefit analyses either before (3 out of 37) or after (4 out of 37) computer matches; authoritative, credible evidence of the cost-effectiveness of computer matching is still lacking; and
- in most Federal agencies, the number of staff assigned to Privacy Act implementation is limited; of 100 agency components responding to this question, 33 reported less than 1 person per agency assigned to privacy and 34 reported 1 person.

Additionally, OTA found that there is little or no governmentwide information on, or OMB oversight of: 1) the scope and magnitude of computer matching, front-end verification, and computer profiling activities; 2) the quality and appropriateness of the personal information that is being used in these applications; and 3) the results and cost-effectiveness of these applications.

Third, **neither Congress nor the executive branch is providing a forum in which the privacy, management efficiency, and law enforcement implications of Federal electronic record system applications can be fully debated and resolved.** The efficiency of government programs and investigations is improved by more complete and accurate information about individuals. The societal interest in protecting individual privacy is benefited by standards and protections for the use of personal information. Public policy needs to recognize and address the tension between these two interests.

Since 1974, the primary policy attention with respect to Federal agency administration has shifted away from privacy-related concerns. Interests in management, efficiency, and budget have dominated the executive and legislative agenda in the late 1970s and early 1980s. Congress has authorized information exchanges among agencies in a number of laws, e.g., the Debt Collection Act of 1982 and the Deficit Reduction Act of 1984. In these instances, congressional debates included only minimal consideration of the privacy implications of these exchanges.

A number of executive bodies have been established to make recommendations for improving the management of the Federal Government, e.g., the President's Council on Integrity and Efficiency, the President's Council on Management Improvement, and the Grace Commission. All have endorsed the increased use of applications such as computer matching, front-end verification, and computer profiling in order to detect fraud, waste, and abuse in government programs. However, these bodies have given little explicit consideration to privacy interests. Some executive guidelines remind agencies to consider privacy interests in implementing new programs, but these are not followed up to ensure agency compliance.

In general, decisions to use applications such as computer matching, front-end verification, and computer profiling are being made by program officials as part of their effort to detect fraud, waste, and abuse. Given the emphasis being placed on Federal management and efficiency, agencies have little incentive to consider privacy concerns when deciding to establish or expand the use of personal record systems. As a result, ethical decisions about the appropriateness of using certain categories of personal information, such as financial, health, or lifestyle, are often made without the knowledge of or oversight by appropriate agency officials (e.g., Privacy Act officers or inspectors general), OMB, Congress, or the affected individuals.

Fourth, **within the Federal Government, the broader social, economic, and political context of information policy, which includes privacy-related issues, is not being considered.** The complexity of Federal Government relations—within executive agencies, between the executive and legislature, between the Federal Government and State governments, and between the Federal Government and the private sector—is mirrored in interconnecting webs of information exchanges. This complexity and interconnectedness is reflected in myriad laws and regulations, most of which have been enacted in a piecemeal fashion without consideration of other information policies.

Some of these policies may be perceived as being somewhat inconsistent with others, e.g., the privacy of personal information and public access to government information. Some laws and regulations may only partially address a problem, e.g., Federal privacy legislation does not include policy for the private sector or for the flow of information across national borders. In other instances, issues that are inherently related and interdependent, such as privacy and security, are debated and legislated in separate forums with only passing attention to their relationship.

Additionally, the Federal Government's information systems, as well as its information policy, are dependent on technological and economic developments. Federal funding for research and development and Federal financial and market regulations will have significant implications for information technologies and markets. Yet, under the present policymaking system, there is no assurance that these implications will be considered. Likewise, the international information policy environment, as well as international technological and economic developments, affects domestic information policy; again, these factors are not systematically considered in the existing policy arenas.

POLICY ACTIONS

OTA identified a range of policy actions for congressional consideration:

1. Congress could do nothing at this time, monitor Federal use of information technology, and leave policymaking to case law and administrative discretion. This would lead to continued uncertainty regarding individual rights and remedies, as well as agency responsibilities. Additionally, lack of congressional action will, in effect, represent an endorsement of the creation of a *de facto* national database and an endorsement of the use of the social security number as a *de facto* national identifier.
2. Congress could consider a number of problem-specific actions. For example:
    - establish control over Federal agency use of computer matching, front-end verification, and computer profiling, including agency decisions to use these applications, the process for use and verification of personal information, and the rights of individuals;
    - implement more controls and protections for sensitive categories of personal information, such as medical and insurance;
    - establish controls to protect the privacy, confidentiality, and security of personal information within the microcomputer environment of the Federal Government, and provide for appropriate enforcement mechanisms;
    - review agency compliance with existing policy on the quality of data/records containing personal information, and, if necessary, legislate more specific guidelines and controls for accuracy and completeness;
    - review issues concerning use of the social security number as a *de facto* national identifier and, if necessary, restrict its use or legislate a new universal identification number; or
    - review policy with regard to access to the Internal Revenue Service's information by Federal and State agencies, and policy with regard to the Internal Revenue Service's access to databases maintained by Federal and State agencies, as well as the private sector. If necessary, legislate a policy that more clearly delineates the circumstances under which such accesses are permitted.
3. Congress could initiate a number of institutional adjustments, e.g., strengthen the oversight role of OMB, increase the Privacy Act staff in agencies, or improve congressional organization and procedures for consideration of information privacy issues. These institutional adjustments could be made individually or in concert. Additionally or separately, Congress could initiate a major institutional change, such as establishing a Data Protection or Privacy Board or Commission.
4. Congress could provide for systematic study of the broader social, economic, and political context of information policy, of which information privacy is a part.

ABOUT THE REPORT

Chapters 2 through 6 of this report provide technical and policy analyses relevant to electronic record systems privacy, and to proposed legislation such as: the "Data Protection Act of 1985" that would establish a Data Protection Board as an independent agency of the executive branch; possible amendments to the Privacy Act and Paperwork Reduction Act; and management improvement legislation.

Appendix A to this report updates trends and issues relevant to the privacy of information in computerized criminal history record systems, the subject of a prior OTA study. Appendix B describes the methodology of and respondents to the OTA survey (known officially as the OTA Federal Agency Data Request). Appendix C lists the OTA contractor papers relevant to this report. Appendix D lists the outside reviewers and contributors. Appendix E summarizes the Deficit Reduction Act regulations on front-end verification. Appendix F describes the privacy and data protection policies in selected countries.

Other components of this OTA assessment include the October 1985 OTA report on *Electronic Surveillance and Civil Liberties* that discusses issues and options relevant to electronic communications privacy, and the February 1986 OTA report on *Management, Security, and Congressional Oversight* that discusses, among other things, management, technical, and legal issues and options relevant to protecting the security (and, hence, privacy) of computer systems.

NATIONAL ASSOCIATION OF TAX ADMINISTRATORS
444 NORTH CAPITOL STREET, N.W., WASHINGTON, D.C. 20001

NATA STATEMENT ON S. 2756 AND ITS EFFECTS ON THE FEDERAL-STATE TAX EXCHANGE PROGRAM

On behalf of the state tax agencies, the National Association of Tax Administrators has prepared this statement to convey to Congress the states' concerns that some provisions of S. 2756, the Computer Matching and Privacy Protection Act of 1986, may have unintended and adverse effects on the Federal-State Tax Exchange Program, a critical element of the state tax enforcement program.

The National Association of Tax Administrators is an organization of the tax collecting agencies of the fifty states and the District of Columbia.

Relevant Provisions of S. 2756

Paragraph (o)(3) in Section 2(b) of the bill would require that individuals whose records are used in matching programs be notified of the matching program. The requirement and the procedures for providing this notice are to be contained in a written agreement that the federal and state agencies involved must enter into at least thirty days prior to the disclosure of the information between them.

Section 5 of the bill provides that no matching agency or non-federal matching entity may take any adverse action against an individual until the agency or entity has independently verified this information. The verification may be from third-party sources or from the individual whose records are matched.

Application of These Requirements to the Federal-State Exchange Program

The notification provision would require IRS or the state tax agencies or both to send notices to each taxpayer informing him of these state matching programs. In its testimony to this Subcommittee, the Office of Management and Budget estimated that, if IRS fulfilled this requirement, these ntoices would cost IRS a minimum of $20 million a year for postage alone. OMB or IRS could seek to have the state tax agencies pay these costs, which would add enormously to the states' cost for participating in the Federal-State Tax Exchange Program. It is conceivable that both IRS and the states would be required to make this notification. It is also conceivable that each taxpayer would have to be notified several times, once for each tape that contains information from his tax returns, even though the same information would appear on each tape.

Description of the Federal-State Tax Exchange Program

The states' use of federal income tax return information dates back to the 1920s when Congress opened this information to the states through a provision in the Revenue Act of 1926. The Federal-State Tax Exchange Program was established formally in the late 1950s with the negotiation of IRS/state tax agency cooperative agreements providing for the exchange of tax return information. Computer matching programs, especially to compare information on the federal and state tax returns, have been in effect since 1967. By 1975, all but three of the states with individual income taxes were receiving IRS information on magnetic computer tapes and most were using this information on an annual basis. Currently every state but Nevada (which has no income tax) participates in the program.

This program plays a critical role in state tax enforcement. The matching of the information from the largest tape exchange, the IRS Individual Master File, produces approximately $100 million in state tax revenue each year.

As part of its consideration of the Tax Reform Act of 1976, Congress undertook an extensive review of all uses of federal tax return information including its use for state tax administration. In its revision and reenactment of Section 6103 of the Internal Revenue Code, Congress specifically provided that the Federal-State Tax Exchange Program be made permanent and codified in federal law. To facilitate the program, it also adopted a provision that states would be allowed to continue to use the federal social security numbers for state tax purposes; without this provision, the computer tape matches would have been severely handicapped.

The Federal-State Tax Exchange Program includes the following principal computer matches of federal and state tax information: the Individual Master File, which is an abstract of information on individual income tax returns; the Individual Returns Transaction File Tape Extract, which provides special information reported on federal individual tax returns; the Business Master File, which contains information from corporation, partnership, and other business tax returns; the Audit Information Management System tapes, which provide the tax agencies information on IRS audits of corporation income tax returns when the corporation has its headquarters in a state different from the state requesting the information; and the CP-2000 tape, which reports income other than wages that the taxpayer did not report and which IRS detected through its program of matching tax returns with the reports filed by the payors of interest and dividends. All these computer matches are used only to discover the non-reporter or underreporter of taxable income.

Present Privacy Protections

Federal law already includes a variety of provisions to protect the privacy and use of information handled under the Federal-State Tax Exchange Program. Section 6103 (p) (4) of the Internal Revenue Code lists various safeguards that state tax agencies are required to maintain as a condition for receiving federal tax information, including prohibiting the disclosure of the information to another agency.

The instructions that accompany federal income tax returns inform the taxpayer that IRS may give the information on the tax returns to the states, the District of Columbia, and U.S. Commonwealths "to carry out their tax laws." A statement on each copy of Form 1040, 1040A, and 1040EZ refers the taxpayer to this page in the instructions. The purpose of the instruction is to alert the taxpayer to the exchange program, while the taxpayer still has the opportunity to file a correct tax return with both IRS and the state tax agency.

Section 6.4 of the Model IRS-State Agreement on Coordination of Tax Administration (as shown in the manual on the exchange program) provides that state tax agencies will publicize, in a manner satisfactory to IRS, that federal tax returns and return information were obtained pursuant to specific authority granted by the Internal Revenue Code.

Since October 1978, the Federal-State Tax Exchange Program, including state compliance with the requirements of Section 6103 and the requirements of the Coordination Agreement, has been monitored by the Internal Revenue Service's Office of Disclosure. This Office of Disclosure is directed by a highly qualified technical staff at IRS national headquarters. In each IRS District and Service Center, a Disclosure Officer is responsible for coordinating and supervising all exchanges of information and state compliance with the exchange programs. Upon completion of the use of the tapes or other information, the state tax agency is required either to return this information to IRS or to destroy it and report its destruction to IRS.

Differences from Other Programs

In reviewing the concerns expressed at the September 16 hearing by the various supporters of S. 2756, it is hard to find any elements in common with the Federal-State Tax Exchange Program. Rather, there are a number of obvious differences between the Federal-State Exchange Program and the description of other programs as they were described in testimony.

(1) Most of the programs relate to the voluntary application for special benefits. The Federal-State Tax Exchange Program relates on both sides to the filing of federal and state tax returns that are required to be filed.

(2) In the other programs, the principal notice to the public is one that is published in the Federal Register. In the tax program, the notice is published in the instructions for the tax forms. Each tax return directs the taxpayer to this information in the instructions. Thus, in contrast with other programs, every taxpayer affected by the Federal-State Tax Exchange Program is already being notified of the use of the tax return information in the program.

(3) In the other programs, diverse types of data are combined and the results are used for programs unrelated to the purposes for which one set of data was gathered. In the tax program, all of the data is tax return information and it is used to verify compliance with federal and state tax laws.

(4) Much of the testimony refers to many of these computer matching programs as new developments. The Federal-State Tax Exchange Program and its principal computer matching programs are long-established programs.

(5) Because many of the other programs are benefit programs, the administrative agency can terminate benefits as soon as the computer matching indicates that someone is not eligible for the benefits that he has been receiving. With the Federal-State Tax Exchange Program, the state tax agency sends a request to the taxpayer asking for an explanation. No action is taken to collect the unpaid tax until the taxpayer has had an opportunity to respond to this request.

(6) The testimony at the hearing reported that federal agencies gave little oversight to the matching programs they were conducting or that were being conducted with data they had supplied. In the Internal Revenue Service, the Office of Disclosures at IRS's national offices and Disclosure Officers in each IRS District actively monitor the Federal-State Tax Exchange Program and other uses of federal tax information.

Conclusion

It is the view of the state tax agencies that S. 2756 would impose requirements that would be highly burdensome administratively to the states and would result in heavy costs that would be severely detrimental to state tax enforcement purposes and would provide no privacy benefits to taxpayers. No privacy benefits will result to taxpayers since the existing forms and instructions already make them aware that federal tax return information is routinely used for state tax enforcement purposes. For this reason, the Federal-State Tax Exchange Program should be exempted from the requirements of S. 2756 and especially from any requirement requiring either the Internal Revenue Service or the state tax agencies to make separate mailings to notify taxpayers of this program.

STATEMENT OF
HUGH V. O'NEILL
FOR THE
SUBCOMMITTEE ON OVERSIGHT
OF GOVERNMENT MANAGEMENT
COMMITTEE ON GOVERNMENT AFFAIRS
UNITED STATES SENATE
IN SUPPORT OF S.2756
THE PROPOSED "COMPUTER MATCHING
AND PRIVACY PROTECTION ACT OF 1986"

SEPTEMBER 26, 1986

Senator Cohen, members of the Subcommittee: I am pleased to respond to your request for my written comments on S.2756, "The Computer Matching and Privacy Protection Act of 1986," and its relationship to information technology and privacy. I strongly support your effort in S.2756 to strike the proper balance, on the one hand, between the legitimate needs of the Federal and State agencies to share computerized information to ensure the integrity of government programs and, on the other hand, fair information practice, privacy and due process rights of individuals. I appreciate the opportunity to present my views and hope my comments will be helpful to the Subcommittee. I am ready to assist you in any way I can.

Allow me to present some background about my involvement in information technology and privacy. I am currently a private consultant. My qualifications and experience include the following:

- More than thirty years of professional experience in the areas of: Policy Analysis, Technology Assessment, Systems Analysis, ADP-Based Management Information and Computing Systems, Management Science/Operations Research, Cost-effectiveness/ Benefit Analyses -- including more than twenty years experience in Privacy/Fair Information Practice, data confidentiality and computer security -- and including several published reports and articles on Technology Assessment, the Privacy Act of 1974, computer data security/privacy/ confidentiality.

- Former President of the American Society of Access Professionals (ASAP) [a professional society whose purposes include fostering understanding and appreciation of principles of fair information practice]. Organized and chaired several ASAP symposia and training panels on privacy/fair information practice, computer matching and computer security.

- Served on/chaired several interagency task forces on: Privacy Act, President's Privacy Initiative and computer security. Participated as a reviewer/ contributor for the recent OTA privacy and computer security reports.

- Former Privacy and Fair Information Practice Officer at HHS. Participated in the development of the 1979 computer matching guidelines -- served as member of the President's Council on Integrity and Efficiency's Long Term Computer Matching Project including participation in development of 1982 guidelines and related instructions and checklists.

In order to give a proper perspective to S.2756, some background information on the development of fair information practice, and computer technology along with relevant conclusions and recommendations are presented.

BACKGROUND OF FAIR INFORMATION PRACTICE

More than a decade ago, an advisory committee to the Department of Health, Education, and Welfare issued a fundamental statement of information policy and practice in a report called "Records, Computers and the Rights of Citizens." The July 1973 report of the "Advisory Committee on Automated Personal Data Systems," found that, at that time, a person's privacy was poorly protected against arbitrary or abusive record-keeping practices. To safeguard the privacy of individuals and in recognition of the need to establish standards of record-keeping practices appropriate to the computer age, the report recommended the enactment, by Congress, of a Federal "Code of Fair Information Practice" for all automated personal data systems.

The five basic principles on which the Code rests are as follows:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him/her is in a record and how it is used.
3. There must be a way for an individual to prevent information about him/her that was obtained for one purpose from being used or made available for other purposes without his/her consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him/her.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

There are certain exceptions to these principles in the interest of some greater need -- a couple of examples:

1. There are times when individuals should not be given access to records on themselves; e.g., in order to protect confidential sources in investigations or in the interest of national security.
2. There are times when other societal goals outweigh the need for privacy, and that in such cases information should be disclosed and used without the consent of the individual for purposes other than the specific purpose for which the information was originally collected; e.g., in compelling circumstances affecting the health or safety of a human being, including life-threatening situations.

A balance must be struck so that all statutes, regulations, and policies controlling personal information incorporate the basic principles of the canon while at the same time permit society's other goals to be effectively and efficiently achieved. Both sets of goals may be achieved by adhering to the principles of due process and openness in the individual and global decision-making process.

Exceptions to the Code's principles should be permitted only when the public at large has been alerted, through congressional or state legislative hearings, notices of proposed rulemaking, open deliberative meetings and through professional literature and the general media. It is essential that interested parties, including the public, be given an opportunity to participate fully in the decision-making process; e.g., the decision to use/disclose classes of information for purposes other than those for which the information was originally collected.

Decisions to make exceptions to the privacy rights guaranteed individuals by the Code's principles should be made only at the highest and most responsible level of government and should take the form of a Federal or State statute, Presidential executive order, order of the governor, or formal rule or regulation, so that the public will be informed fully of any action taken.

The Privacy Act of 1974 was the first legislative step in implementing these principles on the Federal level. At the State level, ten States have thus far enacted a comprehensive privacy protection law--either called a Privacy Act or a Fair Information Practice Act. The ten States are: Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, New York, Ohio, Utah, and Virginia.

Now a few items of information that illustrate the other side of the equation; i.e., the rapid expansion of information technology.

BACKGROUND OF COMPUTER TECHNOLOGY - 1986 AND BEYOND

The following characteristics are relevant:

- Increased speed--more than a billion operations per second and ever larger memory capacity.
- Fifth generation of computers to include artificial intelligence.
- Computer networks--central computers with terminals
- Networks of computers--large central processing systems connected.
- Networks of computerized data banks devoted to a single area of interest.
- Networks of computerized data banks devoted to a variety of interests.
- Personal computers, home computers, word processors operating in both networks and as stand alone machines.
- Both technical and managerial problems with respect to computer security--computer crime on the increase.
- Computer matching used to compare records on millions of individuals in different data banks--operating at various levels of government: Federal, State and local--front-end eligibility verification programs and computer profiling expanding rapidly.
- The connection of government and private sector computerized data banks.

- International computer networks cross the boundaries of national law.

Considerable effort has been expended to attempt to maintain adequate and reasonable safeguards for the use of computerized information systems. The legislative and executive branches have both tried to implement the fair information practice principles. However, there is a need for a continuing and even an increased level of effort, if we are to use the most advanced computer-communications technology and still protect the rights of individuals.

RECOMMENDATIONS

In order to focus on this effort, the following initiatives are presented as a point of departure for 1986 and beyond:

- The drafting of second generation fair information practice statutes (The Privacy Act of 1974 is an example of a first generation fair information practice statute).
- The design of safeguards for computer applications especially for computer matching, front-end eligibility verification and computer profiling -- general safeguards in legislation, more detailed safeguards in regulations and policy statements.
- Enacting Federal legislation and designing model state statutes for computer protection/crime situations.
- The use of computer technology for the implementation of fair information practice principles, examples:

access to an index of personal data files and where appropriate records themselves through remote user terminals, computer techniques to enhance security, and computerized Expert Systems to aid in training and implementation of Privacy Act's requirements.

- Follow-up, audit, evaluation to ensure that practice follows the legislative, regulatory and policy safeguards.
- The establishment of an entity with adequate resources and priority to:
  - -- Assist in the above recommendations.
  - -- Perform long-range planning--trying to "lock the barn door before the horse is stolen."
  - -- Assist in the controlled sharing of computerized information.

In sum, both the entity in the executive branch and the legislative branch should work toward the implementation of a proper balance so that statutes, regulations, and policies controlling personal information incorporate the basic principles of fair information practice while at the same time permit society's other goals to be effectively and efficiently achieved.

From the previous discussion and a review of the bill, it can be seen readily that S.2756 is a significant step forward. It will amend the Privacy Act of 1974 to codify in legislation the safeguard procedures developed in the computer matching guidelines. Provisions of the bill ensure due process protection. It also will assist in managing the Privacy Act functions and obtaining resources through the Data Integrity Boards provision. In addition, it authorizes proper disclosures for computer matching and front-end eligibility verification under certain conditions. Finally, the entire legislative process will be used to ensure openness and balance in producing privacy safeguards while permitting advanced computer technology to be effectively and efficiently used.

SPECIFIC ITEMS FOR DRAFTING MODIFICATIONS TO S.2756 AND ITS LEGISLATIVE HISTORY

The following list of suggestions/recommendations should be used to clarify, improve and complete the thrust of S.2756. Some may require new provisions in the bill, others modifications to the present provisions and still others statments in the legislative history. The list is as follows:

- The Data Integrity Boards should be supported by Privacy Offices modeled after the Defense Privacy Office which has these characteristics:
    - Staffed by several full time professionals without other competing duties such as FOIA.
    - Involved in oversight, policy development and coordination -- not operations such as responding to individual requests for access to records.
    - Uses computer technology support when feasible.

- Notification to individuals that their records may be matched can be implemented in several ways. A judicious choice of methods and frequency should produce effective and efficient procedures. Some examples are the following:
    - -- Specific statements sent with individual payment checks, information flyers, etc.
    - -- Use the Privacy Act (e)(3) provision when information is collected for Federal systems of records.
    - -- Use special statements when collecting information for non-Federal systems.
    - -- Publish in the Federal Register to inform organizations that represent the individuals.
    - -- Use news/communications media -- a professionally organized, systematic campaign including newspapers/magazines, television and radio spots, professional and trade journals and in-house newsletters.
- Include matches which are performed with the assistance of private sector data bases.
- Include matches performed by agency/entity contractors -- as provided for now in the matching guidelines.
- Include cost benefits analyses when relevant for evaluation and planning.
- Include development of information technology to support fair information practice -- computerized access to an index of personal data files and where

appropriate records themselves through remote user terminals/personal computers, computer Expert Systems for training and implementation, and technology to support system security.

- Amend subsection (f) of the Privacy Act, relating to regulations, so that agencies will include details of implementing S.2756 in their regulations.
- Use and/or amend subsections (j) and (k) of the Privacy Act to provide agency exemption of certain systems/matches; e.g., national security, criminal investigations, with close oversight so that the exemptions are not abused.
- Provide for a definitive data base of matches and front-end verification programs -- initial survey including all ongoing as of the effective date of the Act and planned matches with annual updates -- so that various analyses can be performed.
- Clarify the use of the new disclosure provision, proposed (b)(13) of the Privacy Act vs. continued use of the "routine use disclosures" for matches started before the effective date of S.2756 but continuing thereafter.
- Amend the Privacy Act [sec. (e)(3)] provision to require that individuals be given information on potential (b)(13) disclosures.
- Amend the Privacy Act [sec. (e)(4)] provision to require (b)(13) information in the Federal Register system of records notice.

- Include matches performed within the agency when the records or systems of records were not collected for a purpose in any way related or compatible with each other.
- Make clear that the requirements do not include matches done to develop or report aggregate or anonymous information not intended to be used, in whole or in part, for making a decision about an individual that is not an integral part of the particular research project or procedure. One example is certain medical epidemiological research during which computer matches are performed and decisions may be made as part of the overall project or procedure; these matches are not the type of matches that S.2756 is directed toward, but this should be made clear.

CONCLUSION

In sum, I think that S.2756, the Computer Matching and Privacy Protection Act of 1986, is a major contribution to the controlled sharing of computerized information and the protection of individual rights while using advanced information technology. There is need for clarifications, modifications and additions; but, the bill and the subcommittee's hearings are very significant forward steps in the legislative process. I will be happy to be of any further assistance in both the general development or the drafting of specific provisions.

64-697 (368)